國立成功大學

電信管理研究所

碩士論文

大數據隱私議題及我國隱私保護改善方向之探討

The Issues of Big Data Privacy and the Discussion on Improvement Direction of Privacy Protection in Taiwan.

研究生：巫昱德

指導教授：黃郁雯　博士

中華民國一百零七年六月

國立成功大學

碩士論文

大數據隱私議題及我國隱私保護改善方向之探討

The Issues of Big Data Privacy and the Discussion on Improvement Direction of Privacy Protection in Taiwan.

研究生：巫昱德

本論文業經審查及口試合格特此證明

論文考試委員：葉志良

廖俊雄

指導教授：黃郁雯

系(所)主管：陳勁甫

中　華　民　國　107　年　6　月　30　日

Scanned with CamScanner

摘要

國際數據資訊公司(IDC)預測，全球大數據(Big Data)與分析市場規模將在 5 年以內增加一半以上，預計將從 2015 年的 1220 億美元於 2020 年達到 2000 億美元的規模，年成長率為 11.7%。業者利用大數據的分析來規畫並提供服務，卻同時帶來新的隱私風險，因此如何兼顧大數據應用及隱私權保護則成為全球新興的關鍵課題。

本研究之貢獻包含採用創新研究方法，結合法律研究及實證研究，此一作法為過去缺乏之研究方法。本研究包含四個研究目的。首先，本研究透過文獻回顧及比較研究法，彙整大數據特性、相關應用、風險及各國相關政策、大數據世代下關鍵議題，包括「資料蒐集告知困境」、「去識別化與再識別風險」、「刪除權行使的限制或擴張」及「分析結果引發偏誤與歧視」。並彙整各國對於關鍵議題之現況發展、學者意見。研究對象包括歐盟、美國、日本及我國。第二，本研究進一步以實證研究，透過修正式德爾菲法，找出大數據世代下隱私權相關的關鍵議題作為本研究主要研究議題。第三，本研究皆採用 AHP 專家問卷，針對三大關鍵隱私議題，各別列出改善方向，進行專家問卷設計與調查，蒐集專家對於關鍵隱私議題之看法，本次一共發放 20 分專家問卷，回收 19 份，問卷經由 Expert choice 2000 分析後，得出各個議題及改善方向之相對權重值及優先順序。最後，本研究將分析問卷結果，並給予我國立法機構相關建議。

本研究發現，除了「分析結果引發偏誤與歧視」，其餘三大議題皆通過修正式德爾菲法之篩選標準。透過 AHP 層級分析法亦發現，專家認為「去識別化與再識別風險」為重要性最高之隱私關鍵議題，「資料蒐集告知困境」次之，「刪除權行使的限制或擴張」重要性最低。對於「資料蒐集告知困境」議題，專家學者偏好以「部門式」立法，訂定產業特別法，排除個資法告知義務適用範圍；「去識別化與再識別化風險」中，專家學者偏好針對去識別技術加以限制，規定須以包含加入干擾之方式為之；而「刪除權行使的限制或擴張」議題，專家學者則是偏好鼓勵刪除權擴張，但從嚴行使被遺忘權，訂定被遺忘權之檢驗標準。

本研究建議立法機構可將去識別技術限制納入個資法或強制性國家標準中以作為去識別之要求；將業者蒐集個資之告知義務納入產業特別法，如我國目前之保險法 177-1 條。亦建議個資法中納入被遺忘權，並明訂行使之標準從嚴行使特定標準檢驗之。後續研究除可探討我國去識別化如何訂定技術限制細節、探討不同產業於大數據應用下蒐集個資告知義務之狀況、遺忘權行使之標準，亦可針對「分析結果引發偏誤與歧視」進行改善方向之探討。

關鍵詞：大數據、隱私權、個人資料保護法、修正式德爾菲法、層級分析法

A COMPARATIVE STUDY ON BIG DATA PRIVACY AND ITS LEGAL PRACTICE – FROM THE PERSPECTIVE OF INDUSTRY AND ACADEMIA

Yu-Te Wu
Yu-Wen Huang
Institue of Telecommunication Management

Summary

This research is to find out what policies and regulations different countries have adapted and generate experts' opinions towards critical privacy issues. The methodologies include literature reviews, comparative study, modified Delphi method and AHP analysis.

Key word: Big Data; Privacy; Data Protection; Modified Delphi Method; Analytic Hierarchy Process (AHP)

INTRODUCTION

Enterprises provide services by big data analysis; however, it will bring new risks of privacy at the same time. Therefore, balancing both the application of big data and the privacy protection becomes a critical emerging issue.

METERIAL AND METHODS

By literature reviews and comparative study, one major purposes of this research is to find out what policies and regulations different countries have adapted. In addition, this research attempt to identify some essential privacy issues under big data development, utilizing the modified Delphi method. Thirdly, we try to generate experts' opinions towards these four critical privacy issues by AHP analysis.

RESULTS AND DISCUSSION

The result of empirical research is shown as below three table.

Alternatives	Weight	Priority
Execute obligation of notification strictly, adopting an opt-in model.	0.276	2
Add a non-application clause to exclude economically-beneficial big data applications from Personal Data Protection Law regulations.	0.232	3
Refer to the USA, creating new laws for different industries.	0.313	1
Replace a “data-collected supervision orientation” with a “data-used supervision orientation.”	0.180	4

Alternatives	Weight	Priority
Referring to the EU regulations, use inspection criteria and require data controllers to delete original personal data.	0.231	3
Referring to the EU regulations, use inspection criteria but do not require data controllers to delete original personal data.	0.179	4
Referring to the principle of safe harbor in the USA, list personal data deletion items.	0.266	2
Regulate de-identification according to technical restrictions.	0.324	1

Alternatives	Weight	Priority
Refer to EU, modifying the current act to grant data subjects the right to be forgotten.	0.276	2
Referring to Japan, issuing the standard of exercising the right to be forgotten, exercising the right to be forgotten and strictly enforcing it.	0.565	1
Maintain the present conditions, and do not grant the right to be forgotten.	0.158	3

CONCLUSION

This paper concludes in three findings on three critical privacy issues. First, the privacy policies differ from each country. Second, there are three critical privacy critical privacy issues. First, as to the issue of “risk of de-identification and re-identification”,

regulating the technical de-identification standard is considered the most important approach for big data privacy. Secondly, as to the issue of “data collection dilemma”, establishing sectoral regulation and legal obligation for data controller is considered the most important approach. Whereas in the issue of “restriction or expansion of the right to be forgotten”, most experts agreed to introduce the “right to be forgotten” promoted by the current European legislature, however, experts also suggested that such a right should be enforced strictly with certain restriction.

誌謝

經過晝夜奮戰，本論文終於收筆順利付梓成冊。首先感謝指導教授悉心指導，從提案審查到學位考口試，甚至是日本研討會發表，常常陪我討論到半夜。黃教授要指導身為商科背景的我，完成這項結合統計與法律的研究實不容易，學生須從最基本的法制用字開始，到比較各國法律的異同，實為一段艱辛且漫長的路程。除了透過引導式的提點提升學生的思辨能力，也轉介各產業之專家擔任本研究受訪對象，本研究的受訪專家才得以更加多元化。且黃教授所轉介的專家，知識背景皆相當豐富，使本研究的研究結果更具說服力，建議也更加深入。

同時學生亦想感謝內審委員廖俊雄博士、外審老師葉志良博士以及程法彰博士，每項寶貴建議都是本研究不可或缺的元素，在此表示深摯的謝忱。另外，承蒙各領域之填答專家協助填寫問卷的專家的填答與補充建議，不只讓實證研究順利完成，更豐富了本研究的內容。因此也特別感謝各位填答問卷的專家，尤其在專家們事務繁忙的情況下，能得到各位專家的協助，學生更感與有榮焉。雖然受到許多教授、專家的幫助，恐怕未能完全將各位教授所指出的瑕疵進行修正，因此本人願對此論文缺失之處負責。

最後，想特別感謝在研究所期間，不斷在我身邊相互砥礪，作為我心靈支柱的家人、同學及朋友們，你們的支持是我向前邁進的最大動力，也是你們的陪伴讓我的研究所生涯絢麗多彩。我的為學之路才正要展開，但願不會辜負各位的期許，也要不免俗地說一句：「謹以此論文獻給我的至親好友、我的師長們，以及各位曾經幫助我的人。」

目錄

目錄 viii
表目錄 x
圖目錄 xi
第一章　緒論 1
1.1　研究背景與動機 1
1.2　研究目的 3
1.3　論文架構 3
1.4　研究方法 4
第二章　大數據與隱私風險 8
2.1　大數據之特性 8
2.1.1　大量性(Volume) 8
2.1.2　多樣性(Variety) 8
2.1.3　即時性(Velocity) 9
2.1.4　準確性(Veracity) 9
2.1.5　可變性(Variability) 10
2.1.6　價值性(Value) 10
2.1.7　複雜性(Complexity) 10
2.2　大數據相關應用 10
2.2.1　零售及批發商 11
2.2.2　醫療疾病 11
2.2.3　交通運輸 12
2.2.4　金融機構 13
2.3　大數據發展之隱私風險 13
2.4　大數據發展下歐盟與美國當代隱私政策因應 16
2.4.1　大數據發展下歐盟當代隱私政策因應 16
2.4.2　大數據發展下美國當代隱私政策因應 21
第三章　大數據發展下之隱私議題及各國比較 28
3.1　資料蒐集告知困境 29
3.1.1　歐盟於個人資料蒐集之規範 29
3.1.2　美國於個人資料蒐集之規範 30
3.1.3　日本於個人資料蒐集之規範 32
3.1.4　台灣於個人資料蒐集之規範 33
3.1.5　小結 35
3.2　去識別化與再識別風險 35
3.2.1　歐盟去識別化相關規範 39
3.2.2　美國去識別化相關規範 41
3.2.3　日本去識別化相關規範 44
3.2.4　台灣去識別化相關規範 45
3.2.5　小結 46

3.3 刪除權行使的限制或擴張 48
3.3.1 歐盟刪除權之發展 50
3.3.2 美國刪除權之發展 51
3.3.3 日本刪除權之發展 52
3.3.4 台灣刪除權之發展 53
3.3.5 小結 56
3.4 分析結果引發偏誤與歧視 57
3.4.1 美國於分析結果引發偏誤與歧視之看法 57
3.4.2 台灣於分析結果引發偏誤與歧視之看法 59
3.4.3 小結 59
3.5 大數據應用與我國現行隱私法之衝突與可行做法 60
分析結果引發偏誤與歧視 62
第四章 實證研究 68
4.1 修正式德爾菲法 68
4.1.1 文獻回顧 68
4.1.2 問卷設計與專家選擇 69
4.1.3 問卷統計結果 71
4.1.4 小結 71
4.2 AHP 層級分析法 73
4.2.1 AHP 層級分析法介紹 73
4.2.2 建立 AHP 層級架構 77
4.2.3 研究設計與專家選擇 78
4.3 AHP 層級分析法分析結果 82
4.3.1 問卷處理 82
4.3.2 關鍵隱私議題相對權重分析 83
4.3.3 資料蒐集告知困境相對權重分析 84
4.3.4 去識別化與再識別風險相對權重分析 85
4.3.5 刪除權行使的限制或擴張相對權重分析 86
4.3.6 問卷分析 88
4.3.7 小結 89
第五章 結論與建議 91
5.1 結論 91
5.2 建議 94
5.2.1 政策意涵 95
5.2.2 法律意涵 98
5.2.3 管理意涵 98
5.3 後續研究建議 99
參考文獻 101
附錄一 修正式德爾菲法專家問卷 113
附錄二 AHP 層級分析法問卷 116

表目錄

表 2-1 2014 年美國白宮大數據白皮書探討議題整理 14
表 3-1 各項技術去識別化程度 39
表 3-2 HIPAA 之 Safe Harbor 隱私規則規定需要處理的資訊 43
表 3-3 去識別化各國比較 47
表 3-4 各國刪除權現況比較 55
表 3-5 大數據應用下議題與我國現行法規之衝突 60
表 3-6 本研究選擇各個作法之原因 63
表 4-1 修正式德爾菲法議題文獻回顧 69
表 4-2 修正式德爾菲法專家選擇 70
表 4-3 修正式德爾菲法議題篩選結果 71
表 4-4 AHP 隨機指標表 76
表 4-5 AHP 評估尺度 78
表 4-6 AHP 專家問卷訪談對象 81
表 4-7 大數據世代下關鍵隱私議題相對權重排序 84
表 4-8 資料蒐集告知困境改善作法相對權重排序 85
表 4-9 去識別化與再識別風險改善作法相對權重排序 86
表 4-10 刪除權行使的限制或擴張改善作法相對權重排序 87
表 5-1 各國個人資料保護相關規範及現況 93

圖目錄

圖 1-1 德爾菲法研究流程圖 5
圖 1-2 研究流程圖 7
圖 2-1 大數據應用過程產生之關鍵議題 15
圖 3-1《一般資料保護規章》(GDPR)草案告知義務圖形化 30
圖 3-2 資料識別性光譜 37
圖 3-3 HIPAA 隱私規定去識別化流程 42
圖 4-1 AHP 層級分析法流程圖 76
圖 4-2 本研究層級分析(AHP)之架構圖 78
圖 5-1 商業發展及隱私權光譜 91

第一章　緒論

1.1　研究背景與動機

「Big Data」一詞的應用最早出現於 2010 年 IBM 電腦公司[1]所提出，大數據應用指的是組織結合多樣的數位資料庫及資料採礦科技，擷取出隱藏在龐大資料的重要資訊(Rubinstein, 2012)。國際數據資訊公司[2](IDC)預測，全球大數據(Big Data)與分析市場規模將由 2015 年的 1220 億美元，在 5 年以內增加一半以上，將在 2020 年達到 2000 億美元的規模，年成長率則為 11.7%(陳文義，2016)。+

資策會亦預估，我國大數據軟體市場規模，將從 2014 年的 21 億台幣成長至 2017 年的 34 億台幣。資誠[3](PwC)全球資料分析調查 Gut & Gigabytes 報告顯示 2014 年全球約 64%企業應用大數據以做決策(經濟日報，2015)。

Gartner 諮詢公司[4]預測，至 2017 年，將有超過 75%的公司將投資或計畫投資於大數據之應用。美國計算機協會[5]表示，69.6%的企業認為大數據的應用在商業成功與否非常重要甚至是關鍵，而 2014 年僅有 54.4%的企業這般認為，相較之下認為大數據為業界重要關鍵之企業比例上升。有 72%的企業認為應用大數據後超出預期成效。

中國網際網路信息中心[6](CNNIC)於 2016 年發表《2015 年中國網絡購物市場研究報告》，提及數據被稱為 21 世紀的石油，大數據的蒐集及利用已成為新的價值增長點，大數據應用願景雖美好，但對於隱私提出嚴峻挑戰。根據研究報告顯示，約

[1]IBM，全名為國際商業機器股份有限公司，生產及銷售電腦硬體、軟體，是全球最大的訊息技術和業務解決方案公司，並且為系統架構和網路代管提供諮詢服務。

[2]國際數據資訊公司為一 1964 年設立，從事市場研究、分析和諮詢的美國公司，主要針對資訊科技、電信和消費科技。

[3]資誠聯合會計師事務所是由 1970 年創立於台灣之會計師事務所，主要提供稅務、審計及顧客諮詢服務，亦提供財務及管理顧問、人資以及法律服務。

[4]Gartner 是創立於 1979 年一家從事訊息技術研究和諮詢的美國公司，總部位於康乃狄克州的斯坦福。

[5]計算機協會為創立於 1947 年創立之世界性的計算機從業員專業組織，為全球首創科學性及教育性計算機學會。

[6]中國互聯網絡信息中心為經中華人民共和國國務院主管部門批准之網際網路管理和服務機構，成立於 1997 年。

有 42.9%的受訪民眾討厭大數據當前應用，只有 14.3%的民眾享受大數據應用下的個性化服務(中商情報網，2016)。

業者透過大數據提供應用服務，消費者享受服務，但同時也隨時隨地留下自己的數位足跡(Digital Footprints)，抑或是第三方為使用者所留下數據影子(Data Shadows)，皆可能帶來人類社會新的威脅(Koops, 2011)，尤其是對於我們所珍視的隱私價值的侵害，網際網路資料主體隱私顧慮下產生了新的爭議，因此如何兼顧隱私權保護及研究便利是關鍵課題。除此之外，雖然歐洲或美國等皆對於大數據的應用抱持著樂觀態度，且皆將隱私視為大數據應用下之首要考量，但各國皆對於管制及規範有共識亦有分歧(Ybarra, 2011; Schwartz & Solove, 2014; Tsesis, 2014)。

美國白宮所發布之三次《大數據白皮書》，分別為 2014 年「Big data: Seizing opportunities, preserving values」、2015 年「Big data: Seizing opportunities, preserving values」以及 2016 年第三次白「Big Risks, Big Opportunities: the Intersection of Big Data and Civil Right」，其中內容提及大數據應用之價值及所產生之問題，包含大數據應用下，數據之蒐集難以保留去識別及匿名狀態，因再識別化的相關技術進步快速，難以防止再識別化風險。

2014 年所發布之大數據白皮書「Big data: Seizing opportunities, preserving values」內容指出，《消費者隱私權法》草案中賦予人民之主要權利，包含資料主體的控制權、透明化、資料蒐集最小化原則等之探討，大多皆與資料主體對於個人資料刪除權相關。另外也提及業者可應用大數據分析獲取有利資訊，對業者及消費者皆有正面影響。然而，該報告也指出，大數據應用亦可能因為分析結果而產生對消費者特性的偏誤，或者造成對特定公民的歧視。2015 年所發布之第二次白皮書，提及大數據應用下應重新檢視「告知與同意」之框架，並檢討是否應該以此作為隱私保護之基礎。2016 年第三次的白皮書「Big Risks, Big Opportunities: the Intersection of Big Data and Civil Right」，則提出諸多給予聯邦政府之建議，強調應確保大數據應用下人民權利之保護，並應避免人民受到歧視傷害。

因此本研究將針對大數據應用下新興之隱私議題加以探討，並針對我國管制進行分析及建議。

1.2 研究目的

本研究希望藉由國內外文獻整理，分析大數據特性、相關應用、可能所造成的隱風險，以及各國對於大數據發展推展哪些隱私相關之政策，並以大數據從資料蒐集至分析結果之應用過程，說明可能產生之隱私議題，「資料蒐集告知困境」、「去識別化與再識別風險」、「刪除權行使的限制或擴張」以及「分析結果引發偏誤與歧視」，並比較分析、探討我國相較於其他國家及區域差異與不足之處，並透過層級分析法，找出大數據世代下關鍵隱私議題之個資法改善方向，彙整意見並給予我國立法參考依據，因此本研究目的包含以幾點：

一、研究並比較各國對於大數據發展下隱私相關政策或案例。
二、以實證研究，修正式德爾菲法找出大數據世代下關鍵隱私議題，再以層級分析法了解專家對於隱私議題即改善作法之看法。
三、透過實證研究之結果加以綜合歸納，彙整以提供政府立法機構、業者對於大數據發展及隱私保護政策之相關意見。

1.3 論文架構

本研究將包含以下五個章節，其內容之摘要如下：

第一章：緒論，說明研究背景與動機、研究目的、本節之研究架構說明以及研究方法。
第二章：文獻探討，本章節將介紹大數據之發展與特性、相關應用、所產生隱私風險以及各國針對大數據發展之政策推展整理於此。
第三章：本章節針對大數據世代下所產生隱私議題進行研究，探討各國規範及發展。
第四章：本研究以層級分析法為主要研究方法，根據文獻回顧建立層級分析法之架構，以資料特性、資料主體及資料控制者三大構面進行專家問卷設計。
第五章：進行專家問卷訪談，藉由個構面之評估指標進行衡量與分析，並將結果收斂。
第六章：結論及建議，透過彙整專家意見及本研究分析之結果，提供我國業者、立法者及相關機構參考建議。

1.4 研究方法

本研究採用文獻分析法(Document Analysis)、比較研究法(Comparative Study)及修正式德爾菲法(Modified Delphi Method)、層級分析法(Analytic Hierarchy Process)，本章節以四項研究方法分別介紹，說明如何以此協助進行本研究。

一、文獻分析法

文獻分析法為藉由文獻的蒐集、分析及研究來獲得所需資料之方法，對文獻作客觀且有系統地描述的研究方法。文獻分析可以協助研究者釐清研究背景的事實以及研究的具體方向為何，並且協助研究者選擇適合地研究方法，簡言之，文獻分析法可協助研究者了解及重建過去、解釋現在及推測未來(葉志誠等，1999)。本研究為彙整大數據應用之特性、相關應用、風險及相關政策，因此採用文獻分析法作為研究方法之一。

二、比較研究法

根據英國歷史學家湯恩比(1984)所言，當需在兩個或多個事件中，構建出一種關係時，即需要採取提綱挈領的方式進行研究，據此需採用比較研究的方式。
比較研究法針對相同事物之不同層面，抑或是同一性質事物之不同種類，分析研究對象之相同點以及差異點(王玉民,1994)。本研究以相同議題探討不同國家發展及政策，因此採用比較研究法為研究方法之一。

三、修正式德爾菲法

德爾菲法(Delphi Method)為一於 1950 年代初期於美國蘭德公司所發展後廣泛應用於各研究機構之研究方法，為結合質與量之研究方法(阮綠茵等人, 2007)。Murry 與 Hammons(1995)認為德爾菲法的前提為以群體集思廣益後的決策優於個人思考之結果，但也可能因群體溝通等多種干擾因素而影響原有之決策。德爾菲法步驟如下<圖 1-1>

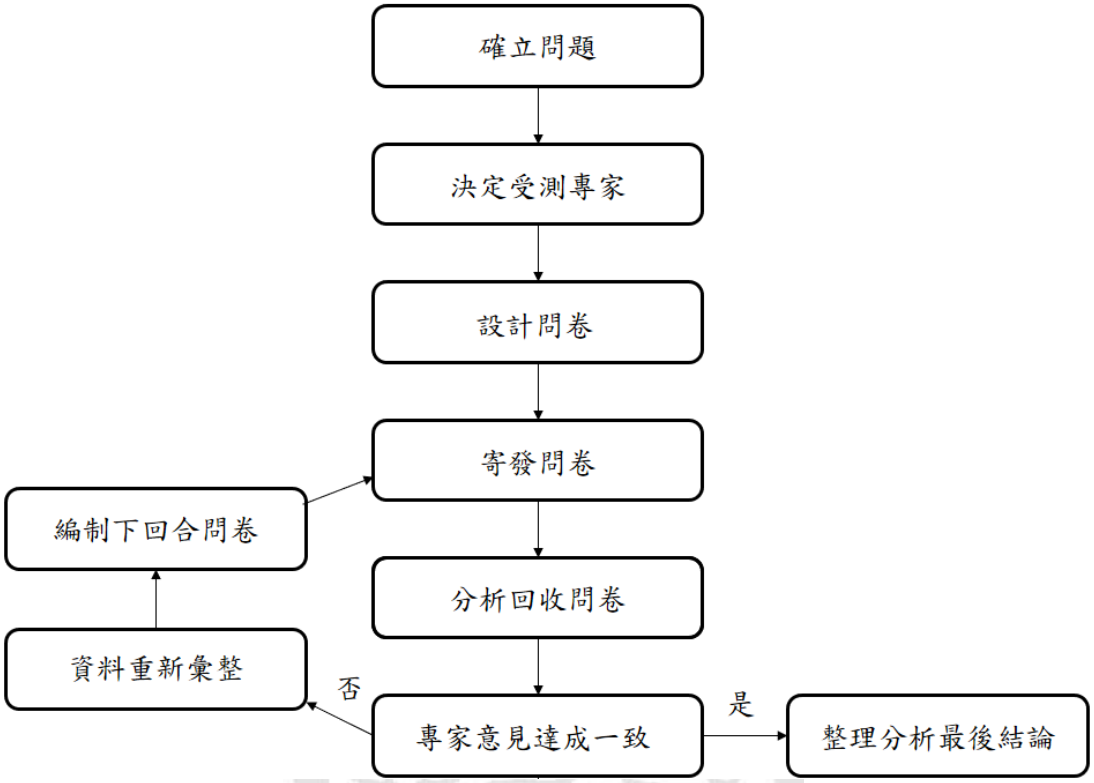


圖 1-1 德爾菲法研究流程圖

資料來源：

由於德爾菲法費時且進度掌控不易，專家意見亦容易產生衝突，Murry 與 Hammoms 於 1995 年提出修正式德爾菲法(Modified Delphi Method)，將傳統德爾菲法之開放性前測部分省略，於第一回合問卷中改採以參考大量文獻發展結構式問卷，可避免耗時之缺點亦可讓問題聚焦收斂。本研究為以實證找出大數據世代下關鍵隱私議題，因此採用修正式德爾菲法為研究方法之一。

四、層級分析法

過去許多研究結合德爾菲法與層級分析法作為主要研究方法，舉凡業者之決策至政府政策訂定，如供應商的選擇(Liao, 2010; Raut, 2014)、保險方案的訂定(Huang, 2008)、國家的進出口政策(Kim, 2012)等。2011 年 Vidal 等學者以德爾菲法為發展基礎之層級分析法之文獻，說明此研究方法如何用以評估複雜決策，即是重要代表之一。

層級分析法是由 Thomas L. Saaty，一位匹茲堡大學教授於 1971 年所提出，其主要目的是以一個層級的結構將複雜問題系統化，由不同的層面給予層級分解，並透過

量化的方法，覓得脈落後分別作比較評估後再整合，可使大型複雜的問題變得比較容易做決策，以提供決策者選擇適當的方案。

當不確定性(Uncertainty)存在於決策過程或包含諸多評估準則時，層級分析法(Saaty, 1980)可協助決策者選擇最佳之決策。由於在複雜的決策過程中，影響決策之因素間常存在著諸多交互作用(Interaction)與抵換關係(Trade-off)，而決策者必須清楚了解各因素間之相對重要性，以萃取出最關鍵之因素。為使不同之專家見解可達到一致性，故 Saaty(1980)發展出層級分析法，使決策過程得以更具邏輯化，幫助決策者解決複雜之問題。

根據 Saaty(1980)研究指出，層級分析法的應用範圍包含

以下十三種情況(沈瑞棋、施東河，1998)：決定優先順序(setting priorities)、產生替代方案(generating set of alternatives)、選擇最佳方案(choosing a best policy alternatives)、決定需求(determining requirements)、資源分配(allocating resources)、預測結果 (predicting outcomes)、衡量績效(measuring performance)、系統設計(designing a system)、確保系統穩定(ensuring system stability)、最佳化(optimizing)、規劃(planning)、解決衝突(conflict resolution)及風險評估(risk assessment)

根據鄧振源、曾國雄研究(1989)，層級分析法之假設包括以下九項：

一、一個系統可以被分類為許多種類或部分，且形成如網路的層級結構。

二、層級結構中，每個層級的要素為獨立性。

三、每一層級內的要素，可用上一層級內某些要素或所有要素作為評估準則，進行比較評估。

四、比較評估時，可將絕對數值尺度轉換成比例尺度(Ratio Scale)。

五、進行成對比較後，可使用正倒值矩陣(Positive Reciprocal Matrix)處理。

六、偏好關係滿足遞移性。不僅優劣關係滿足遞移性，同時強度關係也滿足遞移性。

七、完全具遞移性不容易，因此容許不具遞移性的存在，但需測試其一致性的程度。

八、要素的優勢程度，經由加權法則求得。

九、任何要素只要出現在階層結構中，不論其優勢程度是如何，均被視為與整個評估層級結構有關，而非檢核階層結構的獨立性。

本研究為了解大數據世代下關鍵隱私議題間相對重要性及個資法改善方向作法之相對重要性，因此採用層級分析法為研究方法之一。

本研究之研究流程如下<圖 1-2>：

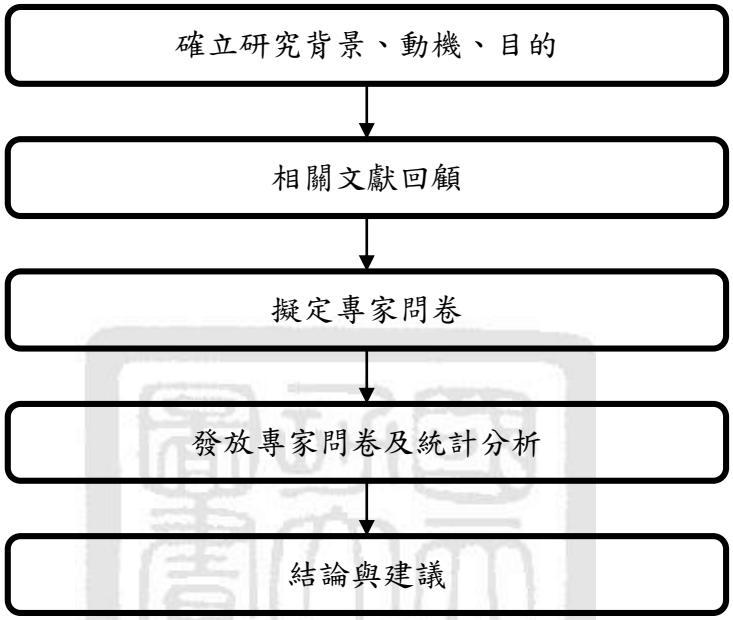


圖 1-2 研究流程圖

資料來源：本研究整理

第二章　大數據與隱私風險

2.1　大數據之特性

國際數據公司(IDC)提出了大數據的四個特徵，包含大量性(Volume)、即時性(Velocity)、多樣性(Variety)以及價值性(Value)，賽仕軟體公司[7](SAS)則提出大數據的兩個面向：可變性(Variability)及複雜性(Complexity) (Davenport & Dyché, 2013)，而 IBM[8]亦提出大量性(Volume)、多樣性(Variety)、即時性(Velocity)及準確性(Veracity)。

綜觀上述，經本研究彙整，大數據擁有「6V1C」特性，分別為大量性(Volume)、多樣性(Variety)、即時性(Velocity)、準確性(Veracity)、可變性(Variability)、價值性(Value)及複雜性(Complexity)，分別如下述所介紹。

2.1.1　大量性(Volume)

過去，業者透過人力取得各種資料，而現今只要透過機器、網路及社群媒體即可以自動化的型態取得資料，由於自動化及連續性的資料蒐集，導致資料的數量相當龐大(Normandeau, 2013)。根據研究預測，至 2020 年將會產生約相當於 2011 年所產生之資料之五十倍，以 Facebook 及 Twitter 為例，每天分別產生 7 Terabytes[9]和 10 Terabytes 之資料 (Aggarwal, 2016)。因此大數據又被稱為「巨量資料」。

由於大數據的大量性，業者得以進行消費者分析並差別取價[10](Varian, 1997; Clemons & Hitt, 2000)。

2.1.2　多樣性(Variety)

資料分為結構化資料及非結構化資料，約僅 10%的可用資料屬於結構化資料，這些資料被存取至特定的資料欄位進行儲存、運算，過去透過傳統管道取得資料多

[7]賽仕(SAS)為一個美國統計分析軟體公司，總部位於北卡羅來納州。
[8]IBM，同前引註 1。
[9]1 Terabyte= 1012 byte. (位元組)
[10]差別取價又稱為價格歧視(Price discrimination)，指商品或服務的提供者提供相同之產品或服務卻對不同族群執行不同之收費標準。

屬於結構化資料，而大數據的多樣性來自於非傳統管道所取得的非結構資料，雖然非結構化資料相當難以處理分析，但它是大數據蘊藏價值的一個相當重要的因素。

Google 能成為大數據技術龍頭，原因之一在於它成功處理非結構化如大量網站、文件檔案，讓資料主體得以快速造訪瀏覽(趙國棟、易歡歡、糜萬軍、鄂維南，2012)。

但相對的，多樣性使得大數據更難以找出隱私疑慮之處，亦使得對網路安全的攻擊更難以預防(Kshetri, 2014)。根據隱私評估機構 Ponemon 調查，只有 23%的民眾相信非結構化資料可以被妥善並安全地管理(2008)，因此大數據之多樣性亦是造成隱私問題原因之一。

2.1.3 即時性(Velocity)

大數據的資料傳輸需相當快速，即時的資料使用才可以發揮其最大的效用，也代表著業者回應這些資料的速度亦成為挑戰之一。廣告商透過即時的點擊串流的存取、便利商店銷售時點情報系統(POS, Point of sales)資料存取，或是知名品牌 Prada 每件衣服上的 RFID 碼，以 RFID 感測裝置以達到即時性，甚至是其他以在地化服務(Location-based)即時存取消費者地理位置。但研究亦顯示資料主體對於即時性的廣告及追蹤科技的隱私顧慮提升，如 Cookies(Cranor, Arjula, & Guduru, 2002; King & Jessen, 2010)。

資料更新的頻率越高，也意味著活性越高，而活性越高價值也越大，在理想的情況下，業者期望當消費者經過實體店家，所接受到的促銷資訊恰巧是消費者所需要的，即可達成雙贏局面，反之，若非為消費者所需要之促銷資訊，除了造成消費者反感外，還浪費了不必要的支出(趙國棟等，2012)。

2.1.4 準確性(Veracity)

準確性最早由美國 Express Scripts 公司的首席數據主管 Inderpal Bhander 提出，因大數據的資料量龐大且雜亂，加深了資料在判別可信度的難度，複雜的資料中亦可能存在人為的錯誤資料或不正確之資訊，尤其在大數據世代下，資料來源過多，且蒐集資料的機構品質不一，因此資料的準確度越來越難以控制。因此從這些龐大

且複雜的資訊中分析出準確的資訊是大數據應用的重要關鍵(Supakkul, S., Zhao, L., & Chung, L., 2016)。

2.1.5 可變性(Variability)

大數據所產生之流量隨著時點不同，而高流量又代表著高隱私風險，如美國大型零售商 Target 在 2013 年 12 月遭受俄羅斯駭客集團攻擊，高達四千萬張信用卡及個人資料曝光，此案例中，俄羅斯駭客集團即是鎖定假日季高峰期最高流量時段進行攻擊(Yadron, 2014)，故大數據的可變性也意味著在不同時點可能產生之隱私風險程度有所不同。

2.1.6 價值性(Value)

從資料中萃取有價值之資料為大數據之特性，亦被認為是最重要之特性，再大數據的應用下，業者們所探討的第一個議題即是所蒐集之大數據有何價值性。《華爾街日報》最近期指出，大部分的業者其實都有這些消費者資訊，卻不知道如何讓這些資訊轉化成有價值的資產(Supakkul, S., Zhao, L., & Chumg, L., 2016)。

2.1.7 複雜性(Complexity)

資料的應用不須具有識別性，因此部分資料的蒐集可不須經過個人授權同意，儘管如此，不具完全識別性之半去識別化資料，甚至是特定已完全去識別化之資料可能透過資料蒐集比對方式進而再識別化(Brill, 2012; ISACA, 2014)，故大數據之複雜性導致去識別以及再識別的爭議產生。

2.2 大數據相關應用

隨著科技進步，大數據的應用越來越廣泛，而應用的目的也隨產業不同有所差異，例如：提升顧客體驗、降低成本、強化精準行銷或改善流程效率等。

大數據的應用隨著產業不同而有所差異，大數據已廣泛應用於零售批發、醫療服務、政府機構、通訊、金融等領域(國政評論，2015)而我國行政院在 2015 年也聲稱除了製造業外，交通運輸、電子商務、金融業、零售業、醫療業在國外已大量以

大數據發展創新服務，這些產業皆為值得發展之方向(中時電子報，2015)。本研究以下針對零售及批發商、醫療疾病、交通運輸及金融機構介紹大數據相關應用。

2.2.1 零售及批發商

自信用卡從 20 世紀中期興起後，消費者的信用卡交易紀錄成為炙手可熱的寶物，行銷商以此分析出消費者偏好與購物行為。雖各別消費者個人資料僅僅少量，依然存在著商業價值，因此部分業者進行大量蒐集消費者個人資料，以利行銷作業或轉售獲利(Mundie, 2014)。而 Walmart 的倉儲管理系統，被視為零售批發商應用大數據的先驅，使供應商能夠隨時隨地掌握個倉庫庫存數量(The Economist, 2010)。Amazon 應用大數據於發展「你可能會喜歡」系統，推薦消費者購買額外商品。業者通常對於消費者具有識別性之資料不是那麼在意，而較在意消費者的特性及區隔(Omer Tene, 2011)。Mckinsey 公司亦提及，零售及批發商可透過大數據追蹤顧客購物行為，包含購物軌跡、駐留時間等。如 Shopkick 平台[11]與上百家通路商合作，這些通路商即可透過 Shopkick 提供之資料做到即時且客製化的推廣，Shopkick 提供資料主體優惠以換取資料。

2.2.2 醫療疾病

根據 Mckinsey 在 2011 年提出之報告(Manyika et al.)指出，美國醫療照護每年獲得高達 3000 億美金的大數據應用成效，其中超過一半來自減少 8%不必要的醫療支出，並且將大數據在醫療上的應用分為五類：

一、臨床應用

大數據在臨床應用上，包含相對療效研究、臨床決策支援系統、醫療資料的透明化、遠距病患監測以及進階分析應用於病患側寫[12]，每年在美國約可替醫療單位節省一千六百五十億美元的醫療支出。

[11]Shopkick 是個購物相關之應用程式，對使用者來說，可以地理資訊及偏好等換取折扣，對合作通路商而言可獲得使用者數據及個人資料。

[12]側寫為針對不同市場區隔的顧客設計不同折扣組合方案，如零售及批發業之精準行銷。

二、保險給付價格訂定

美國每年約可以透過大數據在保險給付價格訂定的應用，省下五百億美元的醫療支出，包含自動化系統(automated systems)以及醫療經濟與結果研究與論質計酬方案(health economics and outcome research and performance-based pricing plans)。

三、精進藥廠或醫療器材公司的研發

美國每年約可以透過大數據在藥廠及醫療器材的研發上，省下一千億美元的支出，包含預測模型(predictive modeling)、透過統計工具與演算法改善臨床試驗設計(statistical tools and algorithms to improve clinical trial design)、藥物不良反應與再定位分析(drug adverse effects and repositioning analysis)、個人化醫療(personalized medicine)以及分析疾病型態(analyzing disease pattern)。

四、開發新商業模式

由於醫療資料庫的數位化，新型態的商業模式也隨之出現，如透過整合相關資料庫(aggregating and synthesizing patient clinical records and claims datasets)或透過線上平台與社群(online platforms and communities)，皆為醫療業利用大數據下所產生新型態之商業模式。

五、公共衛生

過去公共衛生透過監測系統蒐集結構性資料，但透過大數據應用，蒐集大量、非結構性且即時之資料，將有新的突破，例如美國愛荷華大學研究團隊比對 2004 年三月至 2008 年五月 Yahoo 搜尋引擎查詢「流感」相關訊息的擊點數，成功比監測系統早數個禮拜偵測流行疾病的爆發。

2.2.3 交通運輸

政府可利用大數據改善交通環境，透過利用民眾之個人位置資料，用以協助推展交通政策，如路線規劃、大眾運輸建設或交通流量疏通等(Ratti, 2006)。以韓國首爾為例，政府與韓國電信公司(Korea Telecom)合作，用大數據來分析午夜過後人口密集度最高的五個地區，高達 30 億通話紀錄及交通資訊，並於 2013 開始推出午夜公車的服

務(Zahid, 2013; 江美青，2014)。

自動輔助駕駛技術亦是大數據應用的一環，透過資料的應用民眾亦可接收到以地點為基礎的即時性的交通資訊，業者得以提供即時最適路徑，幫助資料主體提升效率(Schmidt, 2011)。

2.2.4 金融機構

根據統計，金融機構導入大數據分析系統，績效約有效增加兩至三成。而金融業應用大數據的層面相當廣泛，將以以下三種應用探討(商業週刊，2014)：

一、顧客關係管理

整合機構本身原有的客戶資料、顧客在電子商務網站的交易紀錄以及其在社群媒體上的行為資料以及其行為等，以擴展對客戶的瞭解。

二、精準行銷

過去行銷人員只能憑經驗推斷促銷活動該鎖定哪些顧客，但銀行產品及服務五花八門，難以精確判斷行銷效果。但透過將倉儲的資料數據分析後，可以實時行銷[13]、交叉行銷、個性化推銷或客戶生命週期管理[14]之方式以提升業績。

三、風險控管

金融機構在進行金融商品的投資及建議時，可透過大數據據分析將投資組合的風險最小化。另外銀行除了可透過顧客資料分析顧客信用額度外，在評估中小企業貸款風險時，亦可將企業財務、銷售、流通及產資等相關資訊分析以量化企業信用額度。

2.3 大數據發展之隱私風險

美國於 2014 年發布之《大數據白皮書》中，除各別探討大數據對於公部門及私部門的應用及益處外，亦各別探討大數據之於公民及消費者的關係，並提出可能產生

[13]根據客戶即時狀況進行行銷，例如客戶當時的所在地、顧客近期消費等資訊來針對地進行行銷。
[14]顧客生命週期管理用以潛在新顧客獲取以及防止舊顧客的流失，如招商銀行建立顧客流失預警模型，將前五分之一高之流失等級顧客加強挽留措施。

之問題。其中對公民產生歧視問題最為嚴重，對消費者則探討對於資料去識別及刪除的要求，且不論是公民或消費者，蒐集資料之告知同意框架必須重新重新檢視。如下表<2-1>。雖然歐巴馬政府並未於《消費者隱私權法》草案中採用「選擇加入」模式之資料蒐集告知同意框架，但其強化了消費者對於資料的控制權及透明度。於而 2015 年發布《大數據白皮書》中，除了指出《消費者隱私權法》草案賦予資料主體對資料的控制權及透明度外，亦提出需加強對於非美國人之資料保護、學生資料蒐集是否用於教育之目的等，最後提及部分資料分析產生之歧視問題。2016 第三次的《大數據白皮書》則是針對大數據演算系統所產生的機會和對公民產生的問題，此次白皮書大部分探討分析偏誤或歧視問題。

表 2-1 2014 年美國白宮大數據白皮書探討議題整理

公民	消費者
分析結果產生歧視	要求資料刪除 要求去識別化
重新檢視告知同意框架	

資料來源：本研究整理

本研究以大數據應用過程說明可能產生之隱私風險，如下<圖 2-1>。資料客體包含個人資料及非個人資料；資料使用則包含蒐集、利用、處理及刪除。

大數據應用前須取得分析母體，不論未來是否進行去識別化，業者於蒐集階段就必須告知資料主體，甚至特定情況下須取得資料主體之同意，即面臨「資料蒐集告知困境」。而資料經過蒐集後，大數據應用則大多將個人資料做去識別化之處理，則成為非個人資料，但由於再識別風險的產生，去識別化的標準越來越模糊，因此本研究將深入探討「去識別化與再識別風險」。其餘具有識別性之個人資料，資料主體則可能行使刪除權而要求資料控制者刪除之，而刪除權的行使有限制及擴張之不同主張，後續章節亦將深入探討「刪除權行使的限制或擴張」。最後不論是非個人資料或個人資料的處理，皆可能具有「分析結果引發偏誤與歧視」的疑慮，因此本研究亦將探討此一議題。

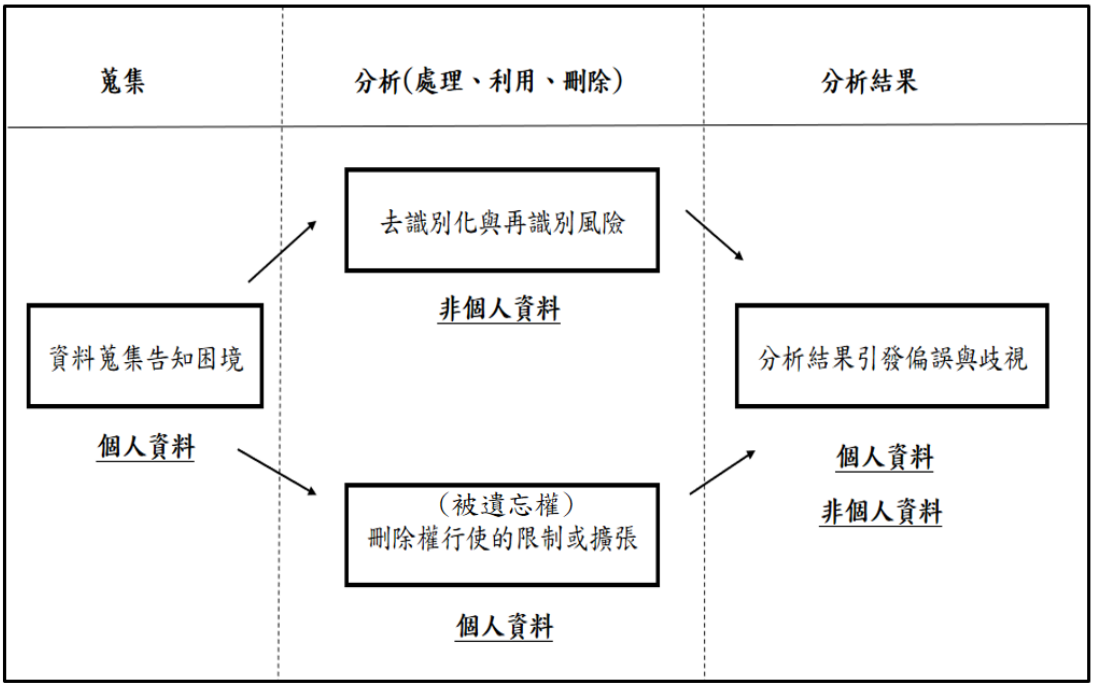


圖 2-1 大數據應用過程產生之關鍵議題

資料來源：本研究自行整理

大數據應用下，帶給人們許多利益，卻也產生隱私風險，大數據的應用下，業者得以精準行銷，良善的精準行銷提升社會福利，但某些精準行銷的應用可能存在道德瑕疵，例如保險業透過精準行銷分析特定顧客可能罹患重症，而要求購買高保費之保險(Drum, 2013)。業者亦可透過非個人資料之數據，以預測較敏感性的個人特性，美國聯邦交易委員會認為這些資料的取得不像敏感性資料不需要授權，但卻能透過大數據預測敏感性資料(Brill, 2012; Danniels, 2013)，例如 Facebook 透過「讚」的交叉分析即可精確預測個人之年齡、種族、宗教、性傾向及政治立場、購物偏好等(Kshetri, 2013)。這種應用模式可能加劇社會階層歧視的問題，弱勢族群可能容易透過資料而被辨認，遭受較負面之待遇(Matturdi, 2014)。

部分業者蒐集資料，並且聲稱這些資料已經過去識別化處理，但這些資料可能經過「再識別化」，識別特定個人，尤其當這些資料可連結至個人的智慧型裝置最具風險(Sweeney,2000; Ohm,2010; Brill, 2012; Jenson,2013)。因此經過去識別化之個人資料被業者再識別化處理也屬大數據應用下隱私風險之一。

2.4 大數據發展下歐盟與美國當代隱私政策因應

大數據應用越趨多元，在科技商業的發展下，各國因此針對大數據相關應用進行政策研擬，而隱私被認為是大數據發展下重要議題(Rubinstein, 2013; Kshetri, 2014)。我國立法院於 2017 年提出資訊長四法並一讀通過，包含《行政院組織法》部分條文修法和《中央行政機關組織基準法》第 23 條修正草案，以及《行政院資訊總處組織法》和《政府資訊機構人員設置管理條例》等 2 項立法提案。資訊長四法之主要目的在於設立專任政府資訊長和資訊總處(iThome，2017)，設立之目的之一即為維護政府資訊安全，可見資訊安全亦漸漸受到重視。過去在隱私法的研究多聚焦於歐盟及美國之政策(Bennett, 1992; Kraus, 1993)。另外，從 2000 年，歐盟執委會與美國政府簽訂《安全港協議》到 2016 年發布的《歐美隱私盾牌協議》皆為國際上具有代表性的隱私保護協議。本研究針對隱私權保護先驅歐盟以及商業自由蓬勃發展之美國兩大指標之隱私政策進行回顧。

2.4.1 大數據發展下歐盟當代隱私政策因應

歐盟資料應用保護的歷史，可從 1995 年歐盟通過《資料保護指令》(European Union Data Protection Directive, 以下簡稱 EU Privacy Directive)提起，其為個人資料保護之最低標準，當時網際網路尚未普及，這些資料種類只包含較簡單的個人資料及數據，歐盟之《資料保護指令》(EU Privacy Directive)雖然為最基本，但也是目前最具影響力的隱私法。此指令確立以下幾大原則(呂雅惠，2007)：

一、資料品質原則

蒐集資料之目的必須明確，處理時不超出目的範圍，且資料須確保正確、隨時更新，亦須以資料主體允許形式保存[15]。

二、正當性原則

唯有在資料主體明確同意下，或為履行契約、法定義務等合法情形之所需，得以

[15]Article 6, EU Privacy Directive.

存取資料主體資料[16]。

三、特種資料原則

規定部分屬於敏感性資料(種族來源、政治取向、宗教、工會會員身分、健康、性生活等)原則上禁止處理，但尚有例外[17]。

四、資料主體相關權益原則

賦予資料主體被告知權，資料處理者須告知資料主體資料處理目的、後果、查詢及更正權等(Article 10)以及請求查詢權、資料刪除及凍結權[18]、以及在特殊或行銷目的將資料轉移下之拒絕權[19]等。

五、資料保管人相關責任原則

要求資料處理人及保管人應確保個人資料之安全性及隱密性、以及相關登記義務及賠償責任。

六、例外及限制原則

規範個資保護例外之情形，如國家安全、犯罪調查等。

網際網路的興起、行動裝置越來越普及、GPS、RFID 的應用發展下，單純以《資料保護指令》(EU Privacy Directive)保護隱私將產生問題，更不用說大數據的應用無法以之確實保障(Kuneret al., 2012)。為了改善隱私法，歐盟在 2002 年 7 月 12 日發布《隱私與電子通訊指令》(Directive on privacy and electronic communications, Directive 2002/58/EC)，明定網際網路業者須採取之措施，以及要求在存取資料主體之資料前必須經過授權，且資料主體有權了解資料之用途，但僅為較粗糙之規範，例如懲處方面並無詳細措施。《隱私與電子通訊指令》(Directive on privacy and electronic communications)要求網站教育資料主體如何啟用、刪除 Cookie，但大部分之業者將此內容放入服務條款或隱私權政策中，而多數資料主體卻無仔細閱讀服務條款及隱私權政策的習慣，因此《資料保護指令》(EU Privacy Directive)及《隱私與電子通訊指令》

[16]Article 7, EU Privacy Directive.
[17]Article 8, EU Privacy Directive
[18]Article 12, EU Privacy Directive
[19]Article 14, EU Privacy Directive

(Directive on privacy and electronic communications)再授權議題無法確實保障資料主體的相關隱私(Cate, 2006)。有鑑於此，2009 年 11 月 25 日，歐盟對資料保護規範又有重要的進展，通過了《歐洲 Cookie 指令》(EU Cookie Directive, Directive 2009/136/EC)，並於 2011 年 5 月 25 日起實施。《歐洲 Cookie 指令》(EU Cookie Directive)要求業者在資料主體使用進入網站以前預設關閉 Cookie 之使用，直到資料主體授權後才予以使用 Cookie 存取資料主體資料，可見《歐洲 Cookie 指令》(EU Cookie Directive)為《隱私與電子通訊指令》(Directive on privacy and electronic communications)的重要補充，加強了資料主體對於自身資料的風險意識，避免業者以將授權請求加入服務條款或隱私權政策之作法使資料主體在不知情的情況下授權(鈦媒體，2016)。

有鑑於上述問題，歐盟在 2012 年提出《保護個人關於個人資料處理及此等資料自由流通規章(以下簡稱：一般資料保護規章)》草案(General Data Protection Regulation, 以下簡稱 GDPR)，整合上述三大指令[20]，並於 2015 年通過歐盟執委會、2016 年通過歐洲議會，此新法使民眾有權在業者之間轉移自己的資料，有權知道自己的資料是否被盜用，相較於《資料保護指令》(EU Privacy Directive)更強調資料主體擁有被遺忘的權利(iThome，2015)。另外，此規章對於向歐盟不同國家提供服務的企業而言，可不必依照不同國家下的不同管制進行調整，將可大幅減輕合規成本[21]，資料保護成為統一式的監管。解決《資料保護指令》(EU Privacy Directive)制定後各成員國間資料保護法律制度不同的問題，統一規定將直接適用於各成員國。

本研究參考國內外文獻將《一般資料保護規章》(GDPR)新增或修改之規範擷取重點整理出以下：

一、適用對象[22]

歐盟原先之資料保護法，只適用於在歐盟境內從事資料處理活動之境外業者，未來，即使並非以歐盟成員國為營業據點，凡提供產品或服務給歐盟成員國居民、或於歐盟境內從事系統性監控等涉及敏感個人資料蒐集活動之境外公司企業皆屬

[20]Directive 95/46/EC、Directive 2002/58/EC 以及 Directive 2009/136/EC.
[21]合規成本指業者為了符合法規管制所負擔的成本。
[22]Article 3, GDPR.

《一般資料保護規章》(GDPR)之適用對象。

二、賦予個人資料較廣定義[23]

擴展解釋個人資料之定義，凡為可直接或間接過濾出特定對象資訊之資料類型，例如網路瀏覽器 Cookies、網路 IP 位址或足以辨識特定個人身分之基因、生物特徵或醫療資料等皆屬於個人資料。

三、知情及同意權[24]

對於資料主體提供資料的授權標準更加嚴格，需在資料主體充分知情的情況下，若有額外資料需要存取，需要再進行額外的單獨說明及授權請求，且若某資料處理已超出服務提供所必須，則不可將同意資料處理作為簽訂合同的條件。另外，雖無禁止將資料主題之授權請求放入隱私權政策內，但該授權若過於隱晦亦無合法性。

四、被遺忘權及刪除權[25]

被遺忘權及刪除權規範在《一般資料保護規章》(GDPR)中共分為：

1.過去已確立的刪除權：當資料主體依法撤回授權或存取方不再有合法理由繼續處理資料時，資料主體有權要求刪除資料。

2.傳統刪除權的擴張：當資料主體成功要求刪除資料時，資料存取方有責任通知處理此資料的其他資料控制者，刪除關於資料主體所主張的個人資料連結、複製件。

五、資料可攜權[26]

資料主體可以隨時將其個人資料從一個服務提供者處轉移至另一個服務提供者，並要求資料蒐集、處理與利用者對以電子化方法持有的個人資料，需使用結構性、通用的格式，以便利並確保後續個人資料可攜性。從目前第 20 條規範看，資料可攜權適用於資料主體提供予資料控制者的資料，因此個人的未經授權之網絡行

[23]Article 4, GDPR.
[24]Article 7, GDPR.
[25]Article 17, GDPR.
[26]Article 20, GDPR.

為是否亦屬於之，尚須待歐盟資料保護委員會解釋之。而目前國際對於「資料可攜」議題，尚未達成共識。《一般資料保護規章》(GDPR)草案一被提出，隨即引發國際間的熱烈探討：反對者認為，此舉無異將形成未來國際間貿易障礙；支持者則從確保使用者權益觀點，認為未來智慧聯網(IoT)環境下，資料可攜性是不可避免的趨勢，賦予資料當事人法律權利，有助於個人資料的保護。各重要國家對歐盟修正草案立場及意見，值得加以探究，以觀察未來法制發展趨勢(李科逸，2014)。

六、反對權(拒絕權)[27]與自動化決策之限制[28]

資料主體除有權利要求業者停止蒐集處理並刪除其個人資料，除非業者可證明其蒐集處理有正當理由，否則不得強制以資料主體不提供個人資料為由而拒絕提供其服務。除此之外，若業者以大數據應用制定其決策，且此決策對消費者有法律效果或其他較重大之影響，消費者則有權知道資料控制者以大數據應用下的決策之分析方式，亦有權拒絕業者以決策對其造成之損害，部分情況則不在此限如下：

1. 係為締結或履行資料主體與資料控制者間之契約所必要者。
2. 係控管者受拘束之歐盟法或會員國法有明文授權，且定有適當之保護措施以確保資料主體之權利及自由及正當利益者。
3. 係基於資料主體之明確同意者。

七、明訂罰則[29]

對於違反資料保護規定者，依據嚴重程度，由歐盟或成員國資料保護主責機關，處以其所屬企業公司年營業額 2%至 4%之行政罰鍰。

八、隱私保護要求、個人化資料保護措施

業者在存取、利用或處理敏感資料時，應確保資料受到保護及個人隱私不受侵犯。大規模且系統性地散佈或處理敏感資料或對於公共區域進行有系統性監控等，當

[27]Article 21, GDPR.
[28]Article 22, GDPR
[29]Article 83, GDPR.

具有侵害個人權利及自由之風險，資料控制者或保管者必須事前進行資料保護影響評估(Data Protection Impact Assessments)，並且需諮詢並採取資料保護官之建議。如法規明確規範，當進行對個人資料特徵系統性評估、大量敏感資料的處理以及對公共領域大規模系統性監控之狀況需做資料保護影響評估。

九、要求企業設立「資料保護官」(Data Protection Officer, DPO)

凡是企業達一定規模(以員工是否超過 250 人為標準)，且核心業務涉及對歐盟公民的個人資料處理，則企業需設立資料保護官(DPO)。而資料保護官需依法履行其職責，若有違反 GDPR 之情形，資料保護官將會被追究法律責任。

整體而言，《一般資料保護規章》(GDPR)賦予資料主體部分新的權利、強化了資料主體的知情權及授權明確性亦賦予資料控制及保管者更大的責任。即使《一般資料保護規章》(GDPR)補足許多過去歐盟對於資料隱私保護未規範之部分，許多學者認為《一般資料保護規章》(GDPR)僅為《資料保護指令》(EU Privacy Directive)之延伸加強版，對此法提出質疑(Rubinstein, 2012)。以《一般資料保護規章》(GDPR)第 17 章被遺忘權規範為例，並未明確定義出如何權衡言論資訊自由及被遺忘權的方式，而只是新增了哪些情況下資料主體可主張被遺忘權[30](Mantelero,2013)。

2.4.2 大數據發展下美國當代隱私政策因應

美國為世界上最早提出隱私權並予以法律保護的國家，早在 1974 年通過《隱私法案》，相較於歐盟傾向以「政府管制」之原則，美國則偏好「自由市場」原則，將企業對於個資使用的問題賦予資料資料主體與資料蒐集者間基於契約自由原則自行協議，或依照不同產業制定個別的法律，並由主管機關頒布相關命令與規則(王慕民等，2015)，例如美國於 1996 年通過《電信法》(Telecommunication Act)，其中第 222 條規範「消費者的隱私保護」，對於電信事業使用用戶資訊的條件制定限制(Cippguide, 2013)。雖然美國無針對大數據應用管制之立法，但業者在資料的應用須遵守業界特定之隱私權規範。分別如下(金元浦，2016)：

[30] 此章明定以下狀況可以主張被遺忘權：1.資料已不再必要，且與當初目的已不相關。2 資料主體撤回授權。3.資料保存期限已過。4.處理方式違法。Article 17, GDPR.

一、保險健康：如受到保護的健康資料之利用，必須符合《健康保險便利和責任法案》(The Health Insurance Portability and Accountability Act of 1996，HIPAA)規範，此法案保障了健康相關資料。

二、金融機構：若欲存取非公開之個人資料，須遵守《金融服務法現代化法案》(Financial Services Modernization Act)，此法案規定金融機構將顧客之資料加以保密，規定資料應儲存在安全隱密之處，且業者應採取特定保護措施來確保資料存儲及傳輸安全。

三、有線電視：《有線通訊隱私權法案》(Cable Communication Policy Act)，禁止有線電視業者尚未取得顧客同意前利用有線系統蒐集顧客的個人資料；《電視隱私保護法案》(Cable TV Privacy Act)，將隱私權保護範圍擴展到錄像帶銷售或租賃公司的顧客。

四、兒童隱私保護：《兒童在線隱私權保護法案》(The Childrens' Online Privacy Protection Act, COPPA)規定網站業者須向其監護人提供隱私權政策告知，並限制對兒童資料蒐集處理方式及原則。

五、消費者信用：《公平信用報告法》(The Fair Credit Reporting Act)為消費者保護法之延伸，規範消費者信用調查機構對消費者信用報告之製作、傳播等須遵守之事項。

六、電信業者：《電信法》(Telecommunication Act)，賦予電信業者須遵守顧客之 資訊保密之義務。

綜觀上述，過去對於資料相關之隱私權保護以授權同意形式進行，且依照產業劃分，但資料蒐集技術之發展使資料可以隱性方式蒐集，產業界限亦趨於模糊，難以分別規範。因此美國白宮於 2012 年簽署工作報告《網路環境消費者資料隱私保護-保護隱私與產業創新政策架構》(A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy)，此報告對《消費者隱私權法》草案(A Consumer Privacy Bill of Right Act)之立法理念進行闡述介紹、強化公平交易委員會(Fair Trade Commission)之權利、促進全球之隱私規範通用性等。主要以三大構面進行規範(金元浦，2016)：

一、告知與授權框架之強化

業者應賦予消費者選擇權以控制業者蒐集之任何資料，對於即使是未與消費者接觸之第三方，若使用資料之用途會影響消費者權益，即須取得消費者授權。業者亦應說明資料種類、蒐集原因及用途、刪除情況、與第三方分享之目的等，並且有權要求業者利用公開個人資料時與提供資料時之說明一致。

二、資料保存與處理之安全責任

業者應評估隱私和安全風險，採取安全措施以防範可能之風險，如，資料非法取得、利用、揭露等，並以合理措施以評估資料是否正確。另外，業者在資料之特定目的下蒐集、利用及處理，並須以安全的形式刪除資料。

三、責任承擔

業者內部需要建立控制和問責機制，更要對消費者和執法機構承擔外部責任。《消費者隱私權法》草案提出了具體的責任事項並加以考核，包含員工行為控制、內部資料使用監督、向第三方公開資料等方面等。

除此之外，《網路環境消費者資料隱私保護-保護隱私與產業創新政策架構》(A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy)亦提出「FTC 隱私權保護執法之強化」(Strengthening FTC Enforcement)，要求美國聯邦貿易委員會(Federal Trade Commission, FTC)據以訂定隱私權保護之執行準則。因此美國聯邦貿易委員會 FTC 三項隱私權執行準則，包含「從設計保護隱私」(Privacy by design)、「簡化選項」(Simplified Choice for Businesses and Consumers)以及「更佳透明化」(Greater Transparency)。「從設計保護隱私」主要要求業者評估資料安全、合理蒐集等保護隱私原則，「簡化選項」則要求業者提供追蹤選擇機制，讓消費者自行選擇是否願意將數位足跡提供給業者(郭戎晉，2013; 蔡柏坤，2013)。

在 2015 年，美國白宮終於發佈《消費者隱私權法》草案(Consumer Privacy Bill of Rights Act)，以擴大消費者資料之保護範圍，包含以下重點(James, 2015; 宋佩珊, 2016)：

一、透明性

業者必須提供資料主體明確之公告，內容包含明確且即時的隱私安全運作，涵蓋如何保存、存取。

二、個人控制

業者應在合理範圍內提供機制，讓資料主體能控制其個人資料之處理，同時也規範應讓資料主體撤銷個人資料使用的授權。

三、注重資料蒐集與合理使用

受規範的公司機構必須依據其明確合理的說明規則來進行個人資料的蒐集、保存與利用。同時，在資料蒐集之特定目的完成後的合理時間內，必須針對所蒐集的個人資料進行刪除或是去識別化。

四、安全性維護

業者必須進行安全風險評估，並且採取合理的資訊安全防護措施以確保資料主體之資料安全性。

五、存取及正確性

業者應給予資料主體合理的存取權利，同時也應在合理範圍內採取措施以維護資料的正確性。

六、隱私維護責任

業者應對員工執行資安教育訓練、進行隱私評估、隱私設計、遵守隱私保護義務以及採取適當的措施來遵循草案之規定。

《消費者隱私權法》草案要求產業發展處理消費者資料的標準或規則，也要求「聯邦貿易委員會」(Federal Trade Commission, FTC)確認產業所制定的 標準或規則必須符合「消費者隱私權法」之規範，包括提供消費者有關其資料如何被收集、使用與分享的明確通知。如果進行消費者資料收集的公司機構違反了「消費者隱私權法」， FTC 將會對其發起法律行動。

除此之外，在 2000 年，為了因應歐盟在 1995 年公布之歐盟之《資料保護指

令》(EU Privacy Directive)要求當第三方國家通過國內法或國際承諾，對個人資料提供充分保護，才允許將歐盟公民個人信息轉移存儲至該國家處理，美國為避免資料隱私因國際上的傳送而受到影響，美國商務部與歐盟執委會合作擬定《安全港協議》(Safe Harbor Agreement)，對於歐盟可提升資料在美國境內的安全性，對於美國可大幅降低企業需事先獲得授權之成本。安全港協議包含以下幾大原則(Ferrell, 2003)：

一、告知(Notice)

業者應告知資料主體其資訊的蒐集及使用目的，業者也必須提供資料主體聯絡、申訴以及向第三方揭露資訊的方式，並且亦須告知資料主體對於自身資料揭露有何選擇。

二、選擇(Choice)

當業者資料的利用目的已與當初資料主體提供資料時的目的不同，資料主體應有選擇權以取消授權，雖在蒐集一般個人資料以「選擇退出」(opt-in)[31]為主，旦對於敏感性資料應提供明確的授權選擇，即為「選擇加入」(opt-in)。

三、轉移(Onward Transfer)

若業者欲將資料主體之資料提供給第三方，必須遵守上述之告知以及選擇原則，同時若作為轉讓資訊的代理人，應確認第三方亦遵守安全港隱私保護原則，例如擬定書面契約，要求第三方至少也要提供相同等級的隱私保護措施。

四、安全(Security)

業者必須採取合理的預防措施，保障資料主體之資料免於遺失、被濫用、受到未經授權的存取、洩露、竄改以及損毀之狀況。

五、資料完整(Integrity)

個人資料必須使用於和當初蒐集的目的上，業者必須確保資料的可靠性，以達成預期合理的使用、並保持正確和及時更新。

[31] 請參照本文 3.1。

六、存取(Access)

資料主體應擁有存取業者所持有個人資訊的權利，而且能夠要求更正、修改或刪除不正確的個人資訊，除非此舉將侵犯到其他人的權利。

七、執行(Enforcement)

業者須有某些機制以確保符合《安全港協議》(Safe Harbor Agreement)之原則，業者必須提供申訴機制以及未遵守原則時，如何處理以及相關處罰措施必須夠明確，以確保組織遵守法規。

《安全港協議》(Safe Harbor Agreement)一直被美國執行，直到 2015 年 10 月 6 日被歐洲法院(European Court of Justice)裁定無效，原因為一樁由一位奧地利之律師 Maximilian 於 2015 年 8 月發起對臉書(Facebook)的集體訴訟，此訴訟包含歐洲、亞洲、拉丁美洲和澳洲五萬多人之響應。而此訴訟則由先登記之兩萬五千人共同提告，控告臉書忽視歐盟對於保護個人隱私權的理念，監控用戶「按讚」的網路行為，此舉侵犯了用戶的隱私權並違反安全港協議(Leo, 2015)。提訴人要求臉書對 2 萬 5000 人個別賠償五百歐元，總共一千兩百五十萬歐元。最後歐洲法院判決 Facebook 敗訴，從此安全港協議失效，對於此判決導致安全港協議的失效，引起相當大的風波，如美國商務部部長 Penny Pritzker 聲稱這是對數位經濟的一大威脅，相當不認同歐洲法院的裁判(Natalia & Sam,2015)。

《安全港協議》(Safe Harbor Agreement)失效後，歐盟及美國為了解決資料傳輸失去法律保障及規範，雙方經過多次協商，在 2016 年 2 月 29 發布《歐美隱私盾牌協議》(EU-US Privacy Shield)，此協議將取代《安全港協議》(Safe Harbor Agreement)，商業用之個人資料送往美國後，將受到與歐盟境內相同的資料保護標準。另外美國亦向歐盟承諾在美國國務院內設置一獨立於國家安全部門外之監察專員，專以處理對於歐盟公民之個人資料問題申訴或諮詢，並要求美國業者須在被申訴後四十五天內處理，或者歐盟公民可以直接向歐盟資料保護機構(DPA)申訴，請歐盟資料保護機構向美國聯邦貿易委員會(FTC)進行協商及處理(Wei ss,2016)。美國商業部將對參與該資料保護協議之業者進行定期檢驗，若有違規，該業者將被從資料傳輸名單中除名。歐盟及美國政府認為此協議不只可以提升數據經濟，且可以使

歐盟及美國的關係更加穩固。然而，歐洲國會議員 Jan Philipp Albrecht 認為此協議亦相當有可能重蹈《安全港協議》(Safe Harbor Agreement)之覆轍，因為《歐美隱私盾牌協議》亦無法律上的強制執行機制，協議基礎只在於美國權威機構的承諾，並且聲稱獨立之監察專員亦難以獨立行事，因監察專員須向美國國務卿報告，另外此協議尚有可不遵守之例外，如滿足必要的國家利益、公共利益或者執法需求[32]。

美國聯邦貿易委員會(Federal Trade Commission, FTC)於 2010 年提出的「資訊安全立法報告」及「消費者隱私保護報告」皆有強調「從設計著手保護隱私」(Privacy by design)之概念。另外，FTC 亦推動「禁止追蹤機制」(Do-Not-Track Mechnism)，讓資料主體可自行選擇是否提供瀏覽紀錄，即數位足跡。

[32] EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE,EU-U.S. Privacy Shield Principles Retrieved From https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf

第三章　大數據發展下之隱私議題及各國比較

有鑑於大數據應用的普及，本研究透過文獻回顧，將過去研究學者認為在大數據應用下之重要議題彙整。

學者 Ann Cavoukian 及 Daniel Castro (2014)指出，「去識別化」(de-identification)在大數據的應用下扮演重要角色。許多學者也主張「去識別化」通常被認為是在兼顧保護個人隱私的前提之下，讓業者得以享有個人資料帶來之好處的方式(Party, 2007; Rubinstein,2008; Garfinkel, 2015)。但也有學者提出質疑，在現今資料的來源越來越多，可以透過多方的資料比對來提升識別能力，且資訊技術、資料辨別能力亦持續進步，因此「去識別化」是否可以成功降低隱私顧慮，尚存爭議(Sweeney, 2000; Ohm, 2010; Garfinkel, 2015)。

Tene & Polonetsky(2012)年指出，數據應用之價值在於累積大量的數據，並從中分析。因此大數據應用與個資法所強調的「資料蒐集最小化」原則有相違背之處。另外，也由於大數據應用的盛行，資訊大多被少數網路巨擘所控制，而這些資訊的蒐集或控制卻未必皆具有正當性，因此資料刪除權議題一躍成為大數據應用的關鍵課題。學者 Bert-Jaep Koops (2011)指出，「被遺忘權[33]」為大數據世代下的重要議題之一，而「被遺忘權」可視為刪除權之擴張，可見被遺忘權或刪除權之行使成為當代探討大數據應用的另一項關鍵課題。

2016 年 1 月 6 日，美國聯邦交易委員會(Federal Trade Commission, FTC)，發布了一份關於大數據應用之研究報告--「Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues」，其中亦指出大數據分析由於資料來源不盡完善，這些本身含有偏誤的資料在經過分析之後所輸出的結果，極有可能造成社會歧視，導致大數據分析應用可能無意間將歧視特定公民。

此外，為保護消費者個人資料及隱私，隱私權相關法令通常會要求資料蒐集人或資料處理人必須遵守一定的「告知」義務。學者 Jensen(2013)指出大數據的大量性

[33] 被遺忘權為一資料主體之隱私權，即資料主體刪除過去於網路上之個人資料，此個人資料多指稱搜尋引擎之搜尋結果，但由於此權利與言論自由及資訊流通自由相抵觸因此尚存爭議，目前僅有歐盟明訂法律規範賦予資料主體此項權利。

使得資料蒐集與處理的「告知作業」產生巨量成本。美國醫學研究機構 IOM 於 2009 年報告亦指出，由於因業者所提供之服務條款或隱私權政策通常較為複雜，消費者亦未必能充分了解其意涵，造成資料蒐集或處理的「告知作業」出現資訊不對稱及知識落差之問題，使得「告知」實際上無法達到保護資料主體的隱私目的，反而僅是將相關責任轉移轉至消費者身上。上述問題皆指出蒐集告知困境成為大數據應用下之挑戰性議題。

綜上所述，本研究針對大數據應用所衍生的四大議題: 資料蒐集告知困境、去識別化與再識別風險、刪除權行使的限制或擴張以及分析結果引發偏誤或歧視，進行深入探討，分述如下。

3.1 資料蒐集告知困境

美國白宮於 2015 年發布之第二次大數據白皮書中指出，有鑑於大數據之應用普及，原有保護資料主體之告知同意框架應重新檢視。告知同意框架包含「揭露」與「同意」雙面向，揭露意指資料控制者應以合理努力向資料主體說明存取個人資料之原因，並使資料主體了解其個人資料如何被蒐集、利用或分享；同意則指在資料主體在對內容了解下，與資料控制者間之意思表示一致(翁清坤，2013)。而原有的告知同意架構下，同意部分包含以「選擇加入」或「選擇退出」之模式。若為「選擇加入」模式，資料控制者須於蒐集、利用或分享前取得資料主體之同意，因此課以資料控制者引誘資料主體放棄權利的負擔。而同意亦可分為明示同意及默示同意，只要一個告知加上資料主體的一個積極作為則屬於默示同意，而明示同意則需要提供資料主體一個選擇進入的選項。而「選擇退出」之模式則是提供資料主體放棄之機會，若資料主體怠於行使此權利，則視為默示同意。若法規以「選擇加入」模式為主，則會加重業者大數應用蒐集告知成本(Tene & Polonetsk, 2012)。反之若法規以「選擇退出」模式，對資料主體之保護有限，因一般消費者可能對隱私權政策或服務條款不甚了解，存在資訊不對稱獲知識落差問題(翁清坤，2013)。

3.1.1 歐盟於個人資料蒐集之規範

若探討歐盟現行法規，2016 年 5 月公布之一般個人資料保護規章，同意形式則是與 1995 年的歐盟《資料保護指令》(EU Privacy Directive)相同，不強制以書面形式。而告知同意是採取選擇加入模式，資料主體必須表示同意，不論是明示同意或默示同意。因此，由資料控制者預先勾選同意並提供資料主體取消勾選的選擇退出模式在歐盟並無效力(林玫君，2017)。

2016 年通過之《一般資料保護規章》(GDPR)，又近一步針對告知義務進行規範，於草案階段新增標準化且圖形化的告知方式，如下<圖 3-3>。雖此圖形化告知方式並未被採用執行，但《一般資料保護規章》(GDPR)中第 12 條第 1 項規定，告知內容應簡潔易懂，並且以淺白詞語為之。

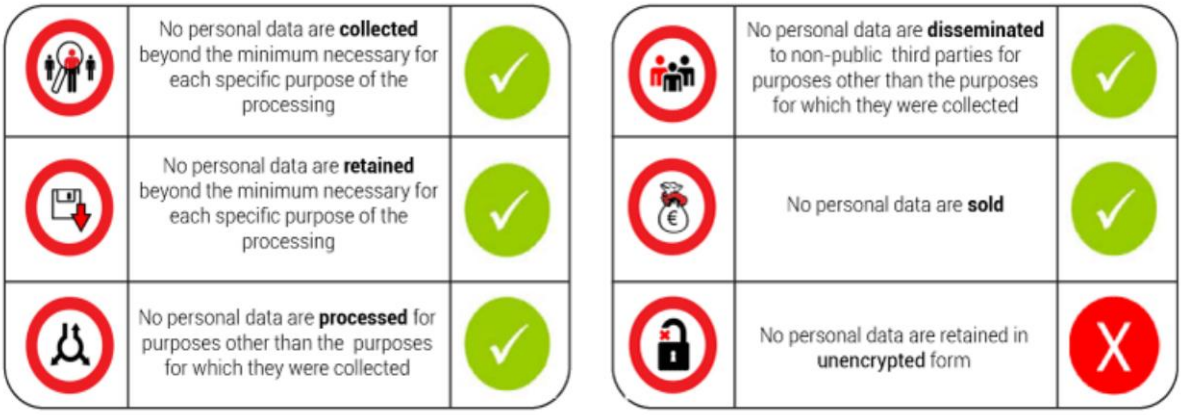


圖 3-1《一般資料保護規章》(GDPR)草案告知義務圖形化

至於德國聯邦最高法院著名的購物回饋案(Das Payback Urteil)判決中，則是認為業者以選擇退出模式蒐集消費者交易資訊等，用以進行精準行銷等市場調查不違法，但若是用以電話、電子郵件等用以廣告目的，則需資料主體的同意，即是以選擇加入模式(林玫君，2017)。

3.1.2 美國於個人資料蒐集之規範

大數據分析下面臨的幾種挑戰，其中之一為蒐集之告知困境，由於大數據大量性[34]，亦是造成難以一一告知資料主體的原因，告知與取得授權的過程可能會產生

[34] 詳見本文 2.1.1

巨量成本(Jensen, 2013)，尤其當現今行動裝置螢幕愈來愈小的趨勢，告知任務將更加困難(Tene & Polonetsk, 2012)。

IOM[35]於 2009 年之報告「beyond the HIPAA privacy rule: enhancing privacy, improving health through research」中，指出由於資訊不對稱之問題，告知實際上無法達到資料主體的隱私保護目的，反而僅是將保護隱私之責任自資料控制者移轉至資料主體，因一般資料控制者所提供之服務條款或隱私權政策通常較為複雜，資料主體亦未必了解內容意涵(Tene & Polonetsk, 2012)。

Kshetri 於 2014 年研究指出，大數據發展下，部分 CSP 業者將以經濟考量而忽略顧客之隱私，如瑞典資料保護權威機構 Datainspektionen 聲稱，Google 在請求授權的服務條款及隱私聲明中，就說明得太過於模糊，保留太多空間 (Tung, 2013)。

根據 2016 年 12 月美國聯邦通訊委員會(FTC)頒布之《電信用戶隱私保護規則》(Protecting the Privacy of Customers of Broadband and Other Telecommunications Services)，規定電信業者於蒐集、利用資料主體敏感性資料時，應以選擇加入(opt-in)模式，即須獲得資料主體同意；但為非敏感資訊，即採用選擇退出(opt-out)模式，除非資料主體拒絕，資料控制者可蒐集利用之個人資料。但 2017 年 4 月 3 日，美國總統川普簽署廢除《電信用戶隱私保護規則》的國會決議，此法規目前已被廢除，原因之一為此法規只僅針對電信業者，但對於大型網際網路業者如 Facebook、Google 等卻無從限制(Cecilia Kang, 2017)。

目前美國採「部門式」個人資料保護模式，即針對不同產業，訂定合適的個人資料保護規範，如電信業之個人資料保護法以 1996 年實施之《電信法》為基礎。聯邦通訊委員會(Federal Communications Commission, FCC)訂定之電信法 222 條要求電信業者保障資料主體資訊自主權，為此 FCC 因此頒布「施行細則」內要求業者「應先取得客戶明示同意」，即「選擇加入」機制，但美國最高法院於 1999 年認定，此規定違反美國憲法增修條文第 1 條所保障之「商業言論」權利[36]。因此 FCC 於 2002 年修改「CPNI 施行細則」，放寬業者之義務，改為「選擇加入」與「選擇退出」並

[35] Institute of Medicine of national academies, 簡稱 IOM，為設立於美國之醫學學術研究機構。

[36] U.S.West, Inc. v. FCC 案，電信業者 U.S.West 於 1999 年對 FCC 提出控訴，指出 CNPI 實施細則以要求業者以「選擇加入」機制蒐集消費者資料，違反憲法第 1 條增修條文保障之商業言論自由。

行制。電信業者與關係企業、代理人、合資夥伴與獨立包商之間基於電信相關服務目的而分享 CPNI，即以「選擇退出」模式即可，包含與合夥投資人、獨立包商等；唯獨分享 CPNI 予非提供電信相關服務的第三方，則要求「選擇加入」同意模式。但 FCC 於 2007 年又修改此細則，稍微擴大業者之義務，僅有電信業者所分享的關係企業係為提供電信相關服務的業者，其同意模式乃採「選擇退出」方式；而分享至第三方或其他非關係企業包含合夥投資人、獨立包商等，皆須以「選擇加入」機制為基礎(翁清坤，2017)。

美國於個人資蒐集、利用及分享，大多部門之法規尚採用「選擇退出」模式，如美國金融服務現代化法(GLBA)明定，金融機構得與第三方共享消費者個人資料，除該消費者主動選擇拒絕其資料之分享。

2000 年歐盟與美國簽訂之「安全港隱私原則」(Safe Harbor Privacy Principle)雖亦以選擇退出(opt out)為基礎，但對於敏感性資料之目的外使用或提供予第三方則須給予資料主體選擇加入(opt in)之權利(翁清坤，2013)。但此原則已於 2015 年因無法有效保護歐盟人民隱私而被廢除，2016 年 2 月 29 發布《歐美隱私盾牌協議》，以協議取代《安全港協議》(Safe Harbor Agreement)。

3.1.3 日本於個人資料蒐集之規範

日本自 2005 年個人情報保護法立法以來，對於個人資料的蒐集皆採「選擇退出」模式，亦即只要當事人對自己資料之被蒐集或利用未行使拒絕權，即視為同意，但資料主體得隨時拒絕資料控制者停止蒐集或利用其個人資料。由於「選擇退出」制度已行之十數年，且過去日本皆有販售個人資料之交易，一般稱之「個資清冊業者」，對經濟發展亦有貢獻，因此修法要求業者於蒐集個人資料時須得到資料主體之同意，修正為「選擇加入」模式，實務上較為困難(范姜真嫩，2014)。

有鑑於上述，日本於 2015 年修正個人情報保護法，加強資料控制者之義務，尤其為提供予第三方之情況，以解決市面上「個資清冊業者」所彙編之產品容易成為非法行銷活動或詐騙利用工具之問題。

2015 年日本各人情報保護法修法後，業者若要將個人資料提供給第三人，亦不須資料主體同意，尚為「選擇退出」模式，儘管尚採用「選擇退出」模式，但相對

過去更加嚴格，須告知資料主體下述內容且使之處於可知悉之狀態(郭戎晉，2016)：

一、第三方名稱及第三方利用之目的

二、提供第三方知方式

三、資料主體請求停止提供第三方之方式

日本個人情報保護法第 18 條第 1 項明確規定，業者於蒐集個人資料時，除非已事先公告個人資料之利用目的，否則應儘快將其利用墓地告知當事人或公告之。雖然需告知資料主體資料使用目的，但並未強制要求資料控制者需「立即」告知。日本個人情報保護法第 27 條第 1 項則是要求業者於「保有」個人資料之義務，應保證下列事項為資料主體可知悉之狀態(郭戎晉，2016)：

一、該當業者之姓名或名稱

二、所有保有個人資料之利用目的

三、請求提供閱覽、請求訂正、提供第三人時，其處理之程序

四、依政令規定有關確保保有個人資料適當處理之必要事項[37]

3.1.4 台灣於個人資料蒐集之規範

我國於 2010 年，立法院正式將電腦處理個人資料保護法[38]，修正為個人資料保護法，為「全面適用式[39]」之法規。我國目前個資法明定，若向當事人蒐集的個人資料，必須告知當事人，甚至需要取得資料主體書面同意，這部分法條直接衝擊大量使用個資的金融等產業，若企業要執行告知義務恐有耗費成本過高的問題(張陳弘，2015;葉志良，2016)。

過度保護資訊隱私權可能對於社會某些權利或利益造成負面影響，因此有利益權衡之必要，因此資訊隱私權的保障應非絕對的，例如我國司法院大法官釋字第

[37] 根據個人情報保護法施行細則第 5 條規定之必要事項包含：關於該當業者保有個人資料當事人不服時之申訴處理窗口、該當業者為認定個人資訊保護團體之成員時，該當認定個人資訊保護團體之名稱及申訴之提出窗口。

[38] 個人資料保護法之前身，1995 年制定，僅限於經電腦處理之個人資料，亦限於法律及主管機關訂定之十幾種特定產業部門，因此亦屬於「部門式」立法。

[39] 相對於散落各產業領域的隱私相關法規(如金控法第 42 條第 1 項及第 43 條第 2 項、銀行法第 48 條第 2 項、電信法第 6 條及稅捐稽徵法 第 33 條)，「個人資料保護法」適用範圍乃最廣，涵蓋公務及非公務機關對 於個人資料的蒐集、處理、利用或分享行為。

603 號解釋：「惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第 23 條[40]規定意旨之範圍內，以法律明確規定對之予以適當之限。」(翁清坤，2013)有鑑於需針對我國目前個資法規範加以探討目前面臨告知同意相關之議題，根據我國個資法第 15 條及 19 條，公務及非公務機關對個人資料之蒐集或處理須告知資料主體且取得同意。本研究整理我國個資法相關規範如下：

一、當蒐集個人資料時，必須明確告訴資料主體之事項

(一)蒐集者名稱。

(二)蒐集目的。

(三)個人資料類別。

(四)個人資料利用期間、地區、對象及方式。

(五)資料主體擁有的權利：查詢、請求閱覽、製給複製本、補充、更正、停止蒐集處理或利用、刪除。

(六)資料主體得自由選擇提供個人資料時，不提供將對其權益產生之影響。

二、不須告知之例外情形

(一)法律明文規定。

(二)個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

(三)告知將妨害公務機關執行法定職務。

(四)告知將妨害第三人之重大利益。

(五)當事人明知應告知之內容。

[40] 憲法第 23 條(基本人權之限制)
以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。

三、告知方式

告知方式不限，只要得以讓資料主體知悉之方式皆可，且蒐集方須自行負舉證責任。

綜觀上述，我國於個人資料蒐集目前是以「選擇加入」為原則，相對於「選擇退出」之設計對資料主體隱私保護較強，但尚有部分情況例外。

3.1.5 小結

針對資料蒐集告知困境，我國其專家建議，我國可參考美國各別訂定產業規範，依業需求訂定不同告知同意之義務，如我國保險法 177-1 條[41]即賦予保險業者為執行核保或理賠作業之需要，於處理利用個人資料得免為告知(吳珞齊，2017; 彭金隆，陳俞沛，孫群，2017)。

除此之外，我國學者亦建議將有利經濟發展之大數據應用排除個資法規範外，如個資法第 51 條規範特定情形不適用個資法規定，或於其他特定條款排除該項規範(吳珞齊，2017; 彭金隆等，2017)。

最後，美國總統科學和技術顧問委員會(President's Council of Advisors on Science and Technology,PCAST)以及 Mayer-Schönberger and Cukier (2013)則是主張以「事後管制」取代「事前管制」。業者雖可自由蒐集消費者之個人資料，但業者將保證資料的利用將不會對資料主體造成任何侵害，若造成任何隱私侵害將由業者負擔相關賠償以及法律責任(吳珞齊，2017; 彭金隆等，2017)。包含美國 2014 年發布之《大數據白皮書》，皆認為應將重點放在使用責任制，讓數據的蒐集者和利用者對資料的管理與其所產生的危害負責，而不應僅將其責任定義為是否通過合理方式蒐集。

3.2 去識別化與再識別風險

[41] 我國個人資料保護法第 177-1 條規定，保險業為執行核保或理賠作業需要，處理、利用依法所蒐集保險契約受益人之姓名、出生年月日、國民身分證統一編號及聯絡方式，得免為個人資料保護法第九條第一項之告知。

國際上一般見解認為，個人資料經過去識別化後，將因無法以合理可能方式識別出特定資料主體，而可迴避個資法的規範限制，進行資料的利用與處理[42]。而傳統之「去識別化」方式為將個人識別性資料去除，僅保留數據。但研究顯示，藉由不同數據間之比對，可將不包含個資之數據透過交叉比對之方式，再識別出特定個人，因此儘管已將資料去識別化，仍會衍生個資與隱私之疑義。如學者 Sweeney(2000)透過投票名單統計發現，約有八成七的美國人擁有唯一的性別、出生日期和郵遞區號，若公開此三項資訊，事實上幾乎等同於直接公開具有識別性之個人。學者 Narayanan, Huey&Felten(2016)提出當前大數據應用下面臨問題，其中之一即為過去透過隱藏個資之去識別化方法，如今已可透過數據比對方式重新辨識特定個人。學者 Paul Ohm 則是認為再識別化造成個人隱私威脅，因此數據應比照個人資料架構管制。

Garfinkel(2015)指出任何資料都在某個識別性光譜<圖 3-2>上，而「去識別化」(de-identification)的動作即是將資料從光譜的右端往左端處理，降低隱私風險；相反地「再識別化」 (re-dientification)則是將資料從光譜的左端往右端處理。Garfinkel 認為若針對資料可否再識別處理，又可將資料分為「匿名化」 (anonymization)資料

[42] 王慕民、陳品安、吳彥欽、張又丹(2015) 主張，雖進行去識別化本身行為仍屬於個人資料的處理，須受到蒐集目的等原則的檢視，但經過去識別化之數據，因不屬於個人資料，故可迴避個資法之規範。

以及「擬匿名化」(pseudonymization)資料，其中，匿名化資料指無法再透過再識別化識別特定人之資料，而擬匿名化資料可透過特定方式再識別化(Garfinkel, 2015)。

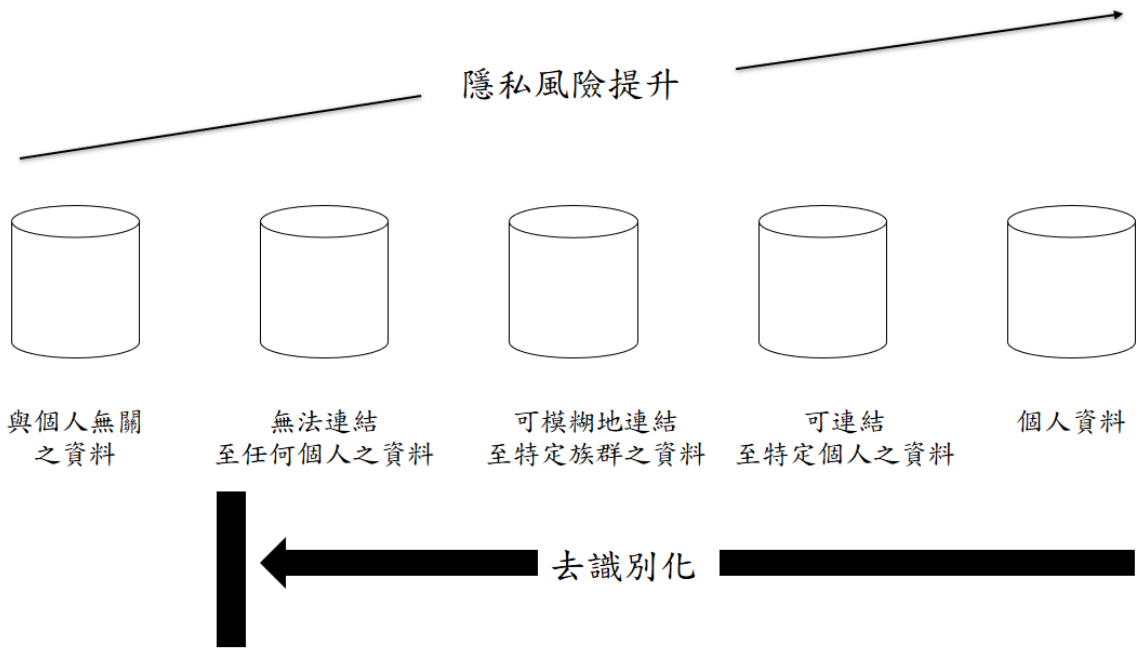


圖 3-2 資料識別性光譜

資料來源：Garfinkel, S. L. (2015). De-Identification of Personal Information.

去識別化方式涵蓋多種技術，較常見的包含資料代碼處理、雜訊加入、取代、K 匿名化、L 多樣性、差異化隱私及資料標記化。本研究參考歐盟第二十九條資料保護小組所提出之意見書，並對各去識別化技術簡單介紹如下：

一、資料代碼化處理(Pseudonymisation)

基本的去識別方式，將個人資料以編碼方式。如：1、2、3、4。

二、雜訊加入(Noise addtion)

將數據添加誤差干擾，以加減或乘積的方式改變數據。例如 Nexflix[43]的資料庫曾經以此種技術去識別處理，但實驗發現只要在選取條件中進一步設定日期條件後，幾乎所有的用戶都可以被識別。

三、取代(Substitute)

[43] Netflix 為於多國提供網路隨選串流影片之企業，且同時於美國經營單一費率郵寄 DVD 出租服務，創立於 1997 年。

將各筆資料數據對調。

四、K 匿名化(K-anonymity)

為避免特定個人在群體中被單獨識別，因此將特定個人與其他具有相同性質的個人列為一組。例如：以國家取代城市。

五、L 多樣性(L-diversity)

改善 K 匿名化技術，確保每筆資料於去識別後有不同之處，但尚存部分再識別機率問題。

六、差異化隱私(Differential Privacy)

目前安全性較高之去識別方法，資料控制者在添加雜訊以後，會從第三方角度常識進行再識別，即使攻擊者擁有相關知識背景或相關資訊，亦可防止其進行再識別。目前較有名之應用如蘋果公司於 2016 年之 iOS10 採用此種技術。

七、資料標記化(Tokeniztion)

以跟原始資料相同之形式將資料亂碼處理。常見於身分證字號的去識別處理。

本章節針對各國對於資料「去識別化」的發展進行探討，以各國對個人資料的定義及「去識別化」的標準為基礎，，另外並彙整部分學者對於「再識別化」風險之研究與建議。

3.2.1 歐盟去識別化相關規範

《歐盟資料保護指令》(EU Privacy Directive)將個人資料的定義為「能用以辨識(identify)特定自然人或具備辨識可能性之任何資料[44]」。根據該指令，具有識別性之個人，指的是個人經由身分證號碼或一個以上專屬其個人身分之因素，包括其個人之身體、精神、心理、經濟、文化或社會地位，可直接或間接被他人所識別[45]。

由眾多歐盟資料保護主管機關(European Union Data Protection Authorities, EUDPAs)所組成的歐盟第 29 條工作小組(The Article 29 Working Party,WP29)曾針對去識別化不同機制進行個案分析，並於 2014 年提出意見書(0829/14/EN WP216)[46]，，作為歐盟去識別化的基本標準。其中，檢驗是否達成去識別化，必須滿足下列三項要求：

一、是否仍可能識別資料主體

二、是否仍可能與其他個人資料相連結

三、是否仍可推論出與特定人相關

比照三項要求來看，若資料接受者即使無法直接經由資料識別特定個人，但若資料原控制者仍保有原始資料，即不符合去識別化規定 (陳聰富、蔡甫昌，2017)。

歐盟規定去識別化的資料，必須達到「完全無從再識別資料主體」之程度，若僅是減少資料主體被再識別的風險，但仍有再識別的可能性，如資料原持有人尚保有原始資料，即不符合「去識別化」的要件，可見 EU 去識別化的要件包括必須刪除原始資料庫，對於去識別化之標準相當嚴格。下<表 3-1>呈現歐盟對於目前去識別化技術是否符合歐盟三大標準之結果：

表 3-1 各項技術去識別化程度

是否達到標準	是否仍可能識別資料主體	是否仍可與其他資料相連結	是否仍可推論出與特定人相關

[44]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 2(a)
[45]Article 2(a) of Directive 95/46/EC
[46]Article 29 data protection working party. Opinion 05/2014 on Anonymisation Techniques. From http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf

去識別化技術	(Is Singling out still a risk?)	(Is Linkability still a risk?)	(Is Inference still a risk?)
資料代碼化處理[47](Pseudonymisation)	Yes	Yes	Yes
雜訊加入[48] (Noise addition)	Yes	May not	May not
取代[49] (Substitution)	Yes	Yes	May not
聚集化或 K 匿名化[50] (Aggregation or K-anonymity)	No	Yes	Yes
L-多樣性(L-diversity)[51]	No	Yes	May not
差異化隱私[52] (Differential privacy)	May not	May not	May not
雜湊/資料標記化[53](Hashing/Tokenization)	Yes	Yes	Maybe

資料來源：歐盟,《Opinion 05/2014 on Anonymisation Techniques》

透過上表，可發現目前尚無任何技術可達到完全無風險之去識別化，業者難以

[47] 資料代碼化為最簡易之去識別化方式，將個人資料部分以編碼取代。
[48] 針對數值型態資料進行加總或乘積擾亂。
[49] 原始資料庫之數值不變，以隨機取代互換方式，通常搭配其他技術一起使用。
[50] 為防止資料主體從人群中被挑出，而將資料主體與 k 個他人為一組，例如以國家取代城市增加相似度。
[51] 改善 K 匿名化之技術，確保同一組內至少有 L 個不同數值，防止推斷攻擊。
[52] 透過雜訊的加入，使攻擊者即使掌握最大背景知識(例如資料庫中 100 筆資料其餘 99 筆)，亦無法推論特定資料之特性。
[53] 將資料變化為另一組同性質資料，如：將身分證字號，置換為另一組符合身分證字號編碼原則的字號，但不是真實資料。

達到此標準。不同於歐盟之規範，英國法院及德國資訊保護官見解則是傾向以資料接受者再識別能力作為判斷標準(我國法務部，2016; 陳聰富&蔡甫昌，2017)，即使資料原持有者未刪除原始資料，也可能符合去識別化標準。但由於英國資料保護法及德國聯邦個人資料保護法中並未有明確去識別化標準，基於歐盟法優於國內法原則，推論英國及德國仍必須遵守歐盟關於去識別化之規範與標準。

3.2.2 美國去識別化相關規範

美國將個人資料定義為「能夠區別(distinguish)特定個人身分或連結(link)到特定個人之資料。」(McCallister et al., 2010)

至於去識別之標準，美國至今沒有一套針對所有產業規範的個人資料保護專法，而是散見於各個產業立法，即「部門式」立法。但美國在判斷資料是否已經過去識別化驗證標準以法令明定的方式，在《醫療保健及責任法案》[54](Health Insurance Portability and Accountability Act)內，最具代表性。《醫療保健及責任法案》明定以「專家判斷法」以及「安全港準則」來判定，若通過驗證標準之個人醫療資訊，即可不須資料主體授權方可使用(Benitez, Loukides & Malin, 2010)，如下圖<3-3>所示，而刪除項目如下表<3-2>所示。

[54] HIPAA 為 1996 年通過的聯邦法律，要求健康保險(包括心理健康醫療)提供者確保患者記錄和健康資訊的隱私，於 2003 年 4 月 14 日生效。

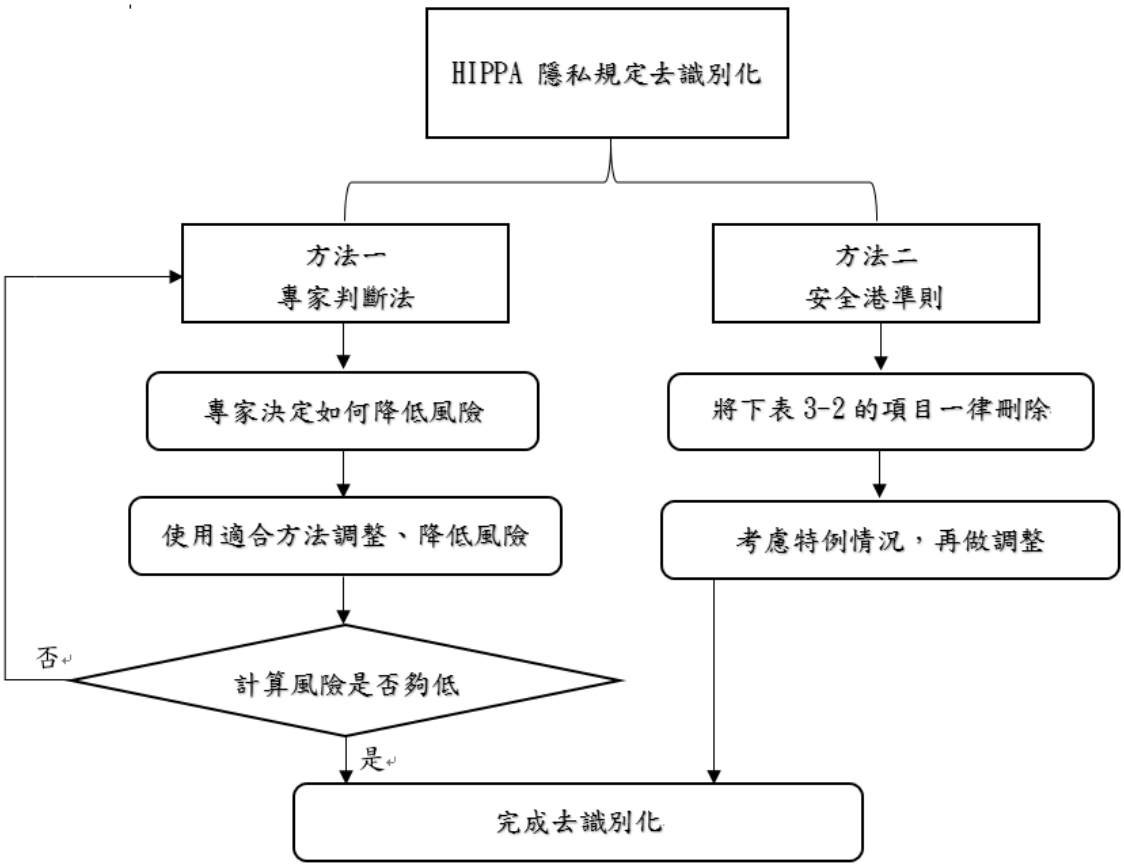


圖 3-3 HIPAA 隱私規定去識別化流程

資料來源：蔡昀臻、樊國楨。大數據之資料去識別的標準化實作初探 ：根基於 ISO/IEC 2nd WD 20889

表 3-2 HIPAA 之 Safe Harbor 隱私規則規定需要處理的資訊

姓名	電話號碼
所有比「州」小的地理單位[55]	直接關係到個人資料的日期[56](年份除外
車輛識別碼和序號，包括車牌號碼	傳真號碼
設備標示符和序列號	電子郵件地址
網頁網址(URLs)	社會安全號碼
通訊協定編號(IP)地址	醫療紀錄編號
生物識別技術，包括指紋和聲紋	健康計劃受益人數
正面照片和任何可比較的影像	帳戶號碼
證照/執照號碼	任何其他唯一識別號，特徵或ж碼等

資料來源：蔡昀臻、樊國楨(2016)。大數據之資料去識別的標準化實作初探 ：根基於 ISO/IEC 2nd WD 20889

專家判斷法之專家一般指在統計、數學或其他科學領域受過去識別化相關教育或有處理過相關事項的人員；專家會透過評估資料的可複製性(Replicability)、資料來源可用性(Data source Availability)、可辨識性(Distinguishability)與風險評鑑(Assess Risk)來決定資料的安全與否，而針對安全港準則有些資料因為情況特殊需要手動調整。例如：如果資料裡面有人的職業是總統，則可能需要另外遮蔽該訊息(蔡昀臻、樊國楨，2016)。研究顯示使用安全港準則，若只留下性別、生日月日以及前三碼郵遞區號，則可將識別性降低於 1%以下(Garfinkel, 2015)。

由上述規範可窺見美國作法為「如何降低再識別化風險」，而並非從「如何完全規避再識別化風險」，美國公民權利辦公室[57]認為無法做到絕對的去識別化，風險值

[55] 包括街道地址，城市、縣、管轄區，郵遞區號，和它們的相對應的地理編碼，而郵遞區號前三碼則根據人口統計局資料調整：如果原來的三碼郵遞區號涵蓋的地理單元人口超過 20000 人;且人口為 20000 以下的地理單元的郵遞區號更改為 000。

[56] 包括出生日期，入院日期，出院日 期，死亡日期；而所有年齡超過 89 歲及其相關日期資料(含年份)合併為「90 歲或以上」之單一類別。

[57] Office for Civeil Right(OCR)，美國公民權利辦公室隸屬於美國健康與人類服務部下，此為維護每

最低狀態為趨近於零並無法等於零，因此只能對風險做評估，因此不同於歐盟訂定實際難以之執行高標準，HIPAA 法採用之專家判斷法及安全港準則皆為降低再識別化風險。

3.2.3 日本去識別化相關規範

為因應日本科技技術快速改變，大數據應用興起，日本於 2015 年大幅修正個人情報保護法(個人情報の保護に関する法律)，新增專責機構「個人情報保護委員會」。此次修法除了修改個人資料定義外，並將「去識別化個人資料(匿名加工情報)[58]」納進個人情報保護法(郭戎晉，2016)。依現行個人資料保護法第 2 條第 1 項，有關生存個人資訊，依包含於其中之姓名、生年月日及其他記述等，而得以識別特定個人者，包含藉由容易組合、比對性之其他資訊，而形成得識別特定個人者。

除此之外，個人資料保護法第 36 條第 1 項明定個人資料去識別化之要求，業者於去識別化處理時，須遵守個人情報保護委員會制定之基準外，於 38 條亦規定不得將其與其他資料比對，亦即禁止再識別之義務。而 36 條第 2 項則是對於個人資料去識別化作業之安全管理如識別性符號外流問題加以規範。而第 36 條第 4 項則課以明示義務，即資料控制者在轉交去識別化資料給第三方時，需明示資料接受者該等資料屬於去識別化資料，以防第三方不須遵守相關規定。第 36 條第 6 項則是對資料控制者課以資料安全維護之義務，資料控制者有致力於採取必要且適當措施並公告該措施內容之義務(郭戎晉，2016)。

相對於歐盟，日本之去識別化定義與我國較為接近，若資料接受者無法再識別特定個人，資料控制者不須將原始資料刪除，亦屬於去識別化資料。但不同之處在於日本除了限制資料控制者必須採用人情報保護委員會規則所定去識別方法，且對資料控制者及資料接受者禁止再識別化的義務，我國則並無相關規範。

國公民健康，並提供公共服務的聯邦政府行政部門。

[58] 日本個人情報保護法第 2 條第 9 項將去識別化個人資料定義為「採取特定措施，對個人情報進行加工處理，使其達到無法識別特定當事人之程度後所產製之相關個人情報，而該等個人資料亦應無法被復原至原始狀態」

3.2.4 台灣去識別化相關規範

我國所定義之個人資料為「指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料[59]。」依其定義反面解釋推論，我國之「去識別化」，指透過一定程序的處理，使個人資料不再具有直接或間接識別性。我國對於資料去識別化與否因得為比對組合之人及資料範圍具有「相對性」，故難有一致性之認定標準，如同個資法施行細則第 3 條修正理由說明所示：「是否得以直接或間接方式識別者，需從蒐集者本身個別加以判斷，此宜於個案中加以審認。」我國法務部自 2014 年 11 月 17 日法務部法律第 10303513040 號函之函釋：「如將公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍。」可見我國法務部亦傾向以資料接受者重新比對再識別的能力判斷達成去識別標準與否，台灣高等行政法院 103 年訴更一字第 120 號判決中，臺北高等行政法院認為，兩者只需其中一方完成即符合個資法之規定；至於個人資料是否已無從辨識該特定個人，則應以資料「收受者」而非「保有者」之角度判斷(樓一琳、何之行，2017)。此見解則與德國資訊保護官及英國法院見解相同，資料收受對象擁有可比對之資料，將不符合去識別化標準，但資料原持有者可不刪除原始資料(蔡昀臻、樊國楨，2016)。

我國行政院分別於民國 103 年及民國 104 年公布去識別化之國家標準 CNS29100 及 CNS29191，範疇涵蓋開放資料及大數據等個人資料，而就 CNS 國家標準而言，必須運用各種技術予以加工處理後，而依其呈現方式達到任何人，甚至包含原資料持有者，皆無法以一切方法，透過資料比對或其他方式再直接或間接辨識出特定個人，但國家標準並無強制性，目前僅為政府機關先行推動，而其他機構或企業可視需要程度在評估驗證導入與否。而法律上判斷去識別化標準，法務部是以「一般人基準說」，意思將可比對之資料定義為公開之資訊，一般人於生活中如報章雜誌等媒體或圖書館等容易搜尋、獲得之資訊，以此作為標準，判斷有無「其他

[59] 個人資料保護法第 2 條。

資訊」作組合、比對之可能(王慕民等，2015)。

3.2.5 小結

本研究將台灣與其他地區比較，彙整出以下<表 3-3>，簡單呈現各國去識別化之標準及差異。

表 3-3 去識別化各國比較

	歐盟	美國	日本	台灣
法規依據	《一般資料處理及流通保護規章》(General Data Protection Regulation, GDPR)	《醫療保健及責任法案》(Health Insurance Portability and Accountability Act, HIPAA)[60]	《個人情報保護法》(個人情報の保護に関する法律)	《個人資料保護法》
發布日期	2012/01/15[61]	1996/08/21	2003/5/23	2010/5/26
個人資料定義	個人資料能用以辨識(identify)特定自然人或具備辨識可能性之任何資料。	能夠區別(distinguish)特定個人身分或連結(link)到特定個人之資料。	有關生存個人資訊，依包含於其中之 姓名、生年月日及其他記述等，而得以識別特定個人者(包含藉由有容易組合、 比對性之其他資訊，而形成得識別特定個人者)。	指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
去識別化標準	以三大標準判斷並要求原始資料一併刪除 ● 是否仍可能識別資料主體？ ● 是否仍可能與其他個人資料相連結？ 三、是否仍可推論出與特定人相關？	明定以「專家判斷法(Expert Determination)」以及「安全港準則(Safe Habor)」為標準來判定。	資料控制者必須採用人情報保護委員會規則所定去識別方法，且經過去識別化之資料，將對資料控制者以及資料接受者課以不得再識別之義務。	需依照資料收受者能力決定達到去識別標準與否。僅有較嚴格之國家標準，但不具強制性。

資料來源：本研究自行整理

美國普林斯頓大學學者 Narayanan 等人除提出大數據應用下隱私威脅外，亦針對傳統去識別化容易被再識別化的問題提出數個解決方式。傳統去識別化方式為「Ad hoc de-identification method」，即以刪除或隱蔽個資之方式去識別化，再識別

[60] 美國於 2015 年歐巴馬政府提出《消費者隱私權法》草案，但於 2016 年川普上任以後，此草案即被擱置。因此目前去識別化標準，最具代表性尚為《醫療保健及責任法案》

[61] 《一般資料處理及流通保護規章》分別於 2015 及 2016 年通過歐盟執委會及國會，預計於 2018 年生效。

風險容易受到取得數據者所擁有資源如其他資料庫所影響。因此三位學者建議須以「Provable privacy method」的去識別化方式，例如差分隱私方法(Differential Privacy Method)，此方式即是需以加入干擾方式，並非傳統將個資刪除或隱蔽之去識別方式，可有效降低再識別化風險。因此三位學者建議立法者應該這種得以確保隱私的技術做為規範標準。

針對在識別化風險，學者 Rapport & Maffi(2013)認為，傳統去識別之方法可透過取得者之既有資料對比識別出特定個人。因此學者建議數據取得應限制特定對象或管道，如禁止匿名者取得資料等。

3.3 刪除權行使的限制或擴張

刪除權可被視為資訊隱私權的一環，根據歐盟《一般資料處理及流通保護規章》(General Data Protection Regulation, GDPR)第 17 條(Article 17)，使用「被遺忘權與刪除權(right to be forgotten and to erasure)」一詞，不同於《資料保護指令》(EU Privacy Directive)中第 12 條之「刪除權(right to access to erase)」，擴大了資料主體可刪除自身個人資料相關連結的權利。因此刪除權包含資料主體對業者提供個人資料之刪除，即「選擇退出(opt out)」，以及資料主體請求搜尋引擎業者刪除自身個人資料之相關連結，即「被遺忘權(right to be forgotten)」。

Tene & Polonetsky 於 2012 年指出，數據應用之價值在於累積大量之數據並從中分析，因此大數據與資料蒐集最小化有相違背之處，應摒棄資料最小化原則，加以限制資料主體之刪除權才得以發揮大數據應用最大價值。

另一方面，部分學者認為大數據世代下第三方更容易取得資料主體的個人資料，認為刪除權應擴張於第三方於網路上轉載資料主體個人資料之相關資訊，如資料主體對搜尋引擎要求其相關資訊刪除之權利(Ohm, 2011; Rosen, 2012)，此概念即為歐盟目前執行之被遺忘權，為刪除權的權利擴張。

然而，亦有反對被遺忘權之學者認為，此類隱私法將限制言論及資訊流通自由，且搜尋引擎業者須負擔刪除連結之營運成本(Rosen, 2012; 顏于嘉，2017)。

Rosen(2012)指出，歐盟執委會委員 Vivian Reding 聲稱被遺忘權核心概念為「若個人不在希望他的個人資料被資料控制者所處理、儲存，且資料控制者沒有合理理由

繼續持有，則資料主體即有權利刪除它。」因此，被遺忘權亦被許多學者認為是刪除權的權利擴張(Ohm, 2011; Rosen, 2012)。歐盟在 2012 年提出之《保護一般資料處理及流通規章草案》中即明確規範了「被遺忘權」[62]，相對於在《資料保護指令》(EU Privacy Directive)中的「刪除權」[63]，擴大新增了第三方(例如搜尋引擎業者)的責任。

我國學者認為，「被遺忘權」與資料的「刪除權」為同一概念，因歐盟於一般《個人資料保護規章》訂定時，以「right to be forgotten and right to be erasure」為名，意味著「刪除權」與「被遺忘權」為不同概念。然而，在該規章立法的一讀程序中，又將之改為「right to be erasure (right to be forgotten)」，學者認為其意味兩者為相同概念，因此 Google 首席隱私顧問 Peter Fleischer 將「被遺忘權」分為三層次來看待(張立翹，2015)：

第一層次：資料主體在網絡上發布了其個人資料相關資訊，資料主體將其刪除之權利。

第二層次：資料主體在網路上發布之個人資料相關資訊被轉載後，資料主體要求其刪除之權利。

第三層次：第三方於網路上發布資料主體個人資料之相關資訊後，資料主體要求其刪除之權利。

「被遺忘權」實施之支持者認為，在大數據世代必要推動的原因為，大量個人資料容易被第三方取得，甚至進而直接揭露於公共領域，並且可長時間保存於在網路上，且只須使用搜索引擎就可輕易被找出來(甄美玲，2016)。因此，應賦予資料主體有行使「被遺忘權」之權利。儘管歐盟執委會執委認為「被遺忘權」為隱私法之新概念，但它卻成為近十年內網際網路及數據應用下相當重要的威脅議題(Rosen, 2012)。被遺忘權的起源於早期的法國，主要適用於更生人的隱私保護，以及部分適用於名譽毀損的案例(Rosen, 2012; Mantelero, 2013)。「被遺忘權」的確立造成言論及資訊自由相當大的威脅(Rosen, 2012)，而業者及媒體在兩種情況下可能侵犯民眾之隱私權--一為揭露個人私事，二為公開公眾之事。在後者情況下，隱私權的保護就須與公共利益互相權衡(Mantelero, 2013)。有學者指出，原始資訊若越老舊，個人被遺忘權的利益就越可

[62] Article 17, GDPR
[63] Article 12, Directive 95/46/EC

能大於公共利益(Weber, 2011)。

3.3.1 歐盟刪除權之發展

歐盟於 1995 年通過《歐洲資料保護指令》(EU Privacy Directive)，其中的 12 章(Article 12)即初次規範了「被遺忘權」的相關概念，根據該規定，當個資不存在必要性時，個人得以要求刪除自己的個人資料[64]。2012 年歐盟公佈《一般資料保護條例草案》(General Data Protection Regulation, GDPR)，第 17 條(Article)明確規定「刪除權(被遺忘權)」[65]，學者認為對於相對於歐盟《資料保護指令》(EU Privacy Directive)的 12 章所稱的刪除權，《一般資料保護條例草案》第 65 條更像是補充在什麼情況下被遺忘權可以行使(Mantelero,2013)。於 2012 年通過並於 2018 實施的《一般資料處理及流通保護規章》，第 65 條即賦予資料主體個人資料刪除權，資料主體得以在資料蒐集或處理目的已無必要、欲撤回當初資料處理所需之同意，或在資料控制者無遵守法規的情況下行使刪除權。第 66 條更是確立被遺忘權的基礎，強調刪除標的可包含搜尋引擎之連結。歐洲法院則是於 2014 年時裁決：當個人資料係「不適當」或「無關連」或「已無關連且多餘」，而且「與公共利益無關」民眾就有權行使被遺忘權(蔣哲宇，2017)。

2014 年在西班牙的一則訴訟「岡薩雷斯訴谷歌公司案」(Costeja v Google Case)則為被遺忘權的關鍵案例，判決結果為谷歌敗訴，該判決對歐盟《資料保護指令》(EU Privacy Directive)作出保護範圍解釋，首次出現判例確立了被遺忘權，個人可要求搜尋引擎業者如 Google 刪除包含其個人資訊之網站連結，但此權利只限於歐盟當地之搜尋引擎，透過其他地區的搜尋引擎尚可搜尋相關資料，因此歐盟第二十九條資料保護工作小組[66](The Article 29 Working Party,WP29)以判決確立的被遺忘權適用性議題，向歐盟法院提出指導意見[67]，希望 Google 將搜尋結果刪除範圍擴大至全球

---

64 Article 12, Directive 95/46/EC

65 Article 17, GDPR
From http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1

66 根據歐盟《資料保護指令》(EU Privacy Directive)第 29 條(Article 29)，由眾多歐盟資料保護主管機關(European Union Data Protection Authorities, EUDPAs)所組成，主要任務為給予歐盟資料保護之建議。

67 Guidelines on the implementation of the court of justice of the European union judgement on "GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/12, Adopted on 26 November 2014 取自 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

搜尋引擎，若位於歐盟使用其他國家版本之搜尋引擎亦無法搜尋到相關資料(Mantelero, 2013; Gilbert, 2015)。而法國法院亦在 2015 年判決 Google 應擴張範圍至全球，要求若搜尋者即使未於歐盟以外國家，透過非歐盟搜尋引擎亦不可搜尋到歐盟人民已主張被遺忘權刪除之資料。但 Google 全球隱私律師 Peter Fleischer 表示，「歐洲法律現在或許規定了被遺忘權，但在全球仍非法定，我們認為，沒有單一國家有權控制另一個國家的人可接觸到的內容。」因此 Google 並未執行，在法國遭罰款 10 萬歐元，並持續上訴中(Xue et al., 2016; Sam, 2016)。

即使於 2014 年，歐盟要求 Google 賦予資料主體被遺忘權，讓 Google 審核資料主體之申請是否通過標準，學者 Jonathan Zittrain 認為執行上尚存在監督風險。若 Google 認為申請未達移除標準，資料主體可以向當地資料保護機關申訴，Google 的判定將會受到行政或司法機關審查。相反的，若 Google 認為申請符合標準，將資料主體個人資料相關連結移除，則僅有當事人及 Google 知道哪些連結已被移除，因此外界無法得知 Google 判斷是否正確，是否存在其他利益衡量(顏于嘉，2017)。

3.3.2 美國刪除權之發展

歐巴馬政府時期，美國白宮在 2015 年 2 月 27 日發布之《消費者隱私權法》(Consumer. Privacy Bill of Rights Act)草案，明確規範資料主體有權利能夠撤銷對資料控制者之授權。但也僅限於自身授權於單一標的之資料，並不包含自身在網路上公開於大眾之資料以及第三方所傳播之資料，且此草案自 2016 年川普上任後至今並無成為法案。

不同於其他國家，美國將資訊隱私權之保障，針對產業分散於不同法規中予以保障，而目前美國並無提供資料主體刪除已公開之個人資訊之權利，即尚未有被遺忘權之概念。

美國憲法第一增修條文已明確規範：「國會不得制定關於下列事項的法律：確立國教或禁止信教自由；剝奪言論自由或出版自由；或剝奪人民和平集會和向政府請願申冤的權利[68](顏于嘉，2017)。」雖然被遺忘權並未被判定為違憲，但許多學者皆認為被遺忘權在美國的引入難度相當高，難以通過憲法第一增修條文之考驗。

[68] U.S constitution First amendment.

另外美國 1996 年通過之《通訊正當行為法》，內容規定：「於第三方發布的信息，任何為之提供技術服務的網絡服務提供者都不應被視為信息的發布者」，亦即搜尋引擎業者提供之搜尋結果不應被視為個人資料的發布者，使得被遺忘權的引入在美國難上加難(彭宏傑、柳雁軍、李瀟璇, 2013)。儘管如此，加州在 2015 年實施的參議院第 568 號法案，Cal. Business & Profession Code § 22580-81，又稱《橡皮擦法案》，賦予未成年者刪除自己過去在網路上任何資訊的權利，原因在於未成年者心智尚未成熟，且網路自我保護意識較弱，在網路上留下的資訊可能造成一輩子的困擾(裴洪輝，2014;Gilbert, 2015)。即使此一法案僅限未成年者自己發部之內容，但此一法律允許未成年者移除個人資資料之原始網站，並非僅是搜尋引擎搜尋結果顯示之連結。因此以刪除內容而言，美國加州之《橡皮擦法案》甚至比歐盟現行之被遺忘權範圍更廣(顏于嘉，2017)。

在 1940 年，曾有一樁判決，Sidis v F-R Publishing Corporation，提告者為一知名數學天才知名兒童，但於晚年生活他為投入於數學研究領域並且過著平凡生活，但新聞媒體尚持續報導他的私生活，當時美國法院認為由於其尚屬公眾人物，大眾對公眾人物有知的權利。而這則判決並不代表絕對的不允許個人刪除自身個人資料，而代表著被遺忘權的行使需以公眾利益及私人利益互相權衡(Mantelero, 2013)。

3.3.3 日本刪除權之發展

日本於 2003 年訂定並於 2005 年實施之《個人情報保護法》，其中賦予資料主體對資料控制者之資料刪除權，凡符合以下條件即可要求資料控制者移除個人資料(范姜真媺，2014)：

一、個人資料內容與事實不符[69]

二、為超越特定利用目的為個人資訊之處理[70]

三、以詐欺、其他不正當方法蒐集個人資料[71]

From https://www.law.cornell.edu/constitution/first_amendment

[69] 日本個人情報保護法第 29 條第 1、2 項規定。

[70] 日本個人情報保護法第 30 條第 1、2 項規定，違反本法第 16 條超越特定利用目的為個人資訊之處理。

[71] 日本個人情報保護法第 30 條第 1、2 項規定，違反本法第 17 條以詐欺、其他不正當方法蒐集個人資料。

四、未得到當事人同意將個人資料提供給第三人[72]

2014 年 1 月，一位日本公民向東京法院上訴，聲稱若在 Google 搜尋引擎打上他的名字，則會錯誤地出現犯罪相關之關鍵字，但法院認為此損害並不超過 Google 以及其他使用者的權益。直到，2014 年 10 月，日本東京法院命令 Google 必須刪除有關過去犯罪紀錄之搜尋結果，此判決可視為日本被遺忘權之首例(Gilbert, 2015)。

2016 年 2 月，日本法院承認「被遺忘權」，上訴者在 2013 年前因違反《禁止兒童賣春和兒童色情法》被判罰款 50 萬日圓，犯罪相關的資料，在 2016 年仍可透過 Google 搜尋引擎找到。該男子以「搜尋結果妨礙他改過自身」，主張「被遺忘權」，要求 Google 刪除有關記錄。埼玉地方法院法官認為：「因犯罪而被大眾所認識的人，亦有被尊重隱私、重新做人的權利。」法官認為當事人犯罪已有 3 年多，搜尋記錄可能妨礙他平靜的生活，所以判處應予刪除(Gilbert, 2015; 彭宏傑等人，2016)。但此案於 2017 年 1 月又遭最高法院以侵害言論自由駁回[73]。而後東京法院對被遺忘權基準做出定義，標準相對嚴格如下(蔣哲宇，2017; Machiko & Mistale, 2017)：

一、報導的事實性質及內容

二、事實傳達的範圍及隱私受害程度

三、當事人的社會地位及影響

四、報導的目的及意義

五、社會的狀況

六、報導中公開當事人真實姓名及住址的必要性

由上述案例可知，被遺忘權在日本即使尚未明確法律規範，但已有確立被遺忘權之判決案例(Chiba, 2016)及評斷基準。

3.3.4 台灣刪除權之發展

雖然我國目前個人資料保護法中具有資料刪除權規定，但刪除權目前解釋上只限於該資料有超越原蒐集個人資料之特定目的必要範圍或期限之情形，因此基

[72] 日本個人情報保護法第 30 條第 1、2 項規定，違反本法第 23 條第 1 項或第 24 條規定，未得到當事人同意將個人資料提供給第三人時。

[73] 日本平成 28 年 45 號判決

本上並以之作為被遺忘權請求基礎難度較高(李思瑩，2016)。如我國目前個資法第11條規定，個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

台灣首樁被遺忘權相關訴訟案例於2014年間，上訴人過去涉及打假球案，而他被起訴後被判無罪，多年來卻可以在搜尋引擎上搜尋到類似資訊。因此施先生於2014年向台灣Google提出告訴，最後於2015年被我國法院宣告敗訴，原因在於法院認定台灣Google並非經營搜尋引擎網站 (Google Search) 之美國公司Google Inc.，其為Google集團所持用之美商Goog1e International LLC在台分公司，因而駁回訴訟，可見被遺忘權在台灣亦尚未被確立(張志偉，2017)。

台灣目前雖無被遺忘權之規定，但對於數據處理，我國目前《個資法》第3條規定有提供近用、修正、停止利用、刪除資料的權利，第11條有個人資料更正或補充等權利，當資料控制者違反《個資法》19條[74](公務機關則為第15條[75])，或特定目的的消失或期限屆滿，資料主體得以請求資料控制者刪除其個人資料。相對於歐盟《一般資料保護規章》，除了當事人參與資料刪除程度較低外，與歐盟規定相對照，罰鍰金額相當懸殊(石世豪，2014)。

---

[74] 台灣個人資料保護法第19條規定非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
一、法律明文規定。
二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
五、經當事人同意。
六、為增進公共利益所必要。
七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
八、對當事人權益無侵害。
蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人
資料。

[75] 台灣個人資料保護法第15條規定公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
一、執行法定職務必要範圍內。
二、經當事人同意。
三、對當事人權益無侵害。

本研究將台灣與其他地區比較，彙整出以下<表 3-4>，簡單呈現各國刪除權之發展。

表 3-4 各國刪除權現況比較

	法規依據	發布日期	資料主體行使選擇退出(opt out)權之條件	資料控制者刪除已公開資料(或連結)之評估條件	已公開資料刪除標的
歐盟	《一般資料處理及流通保護規章》(General Data Protection Regulation)	2012/1/15	●蒐集或處理之目的已無必要 ●當事人撤回處理資料所需之同意 ●資料控制者無遵守法規	●「不適當」或「無關連」或「多餘的」且與公共利益無關	●刪除連結不刪除原始資料
美國	《加州商業及職業法》(Cal. Business & Profession Code § 22580-81)	2013/10/1	無相關法規	●資料主體未成年	不僅刪除連結刪除原始資料
美國	《電信法》(Telecommunications Act)	1996/2/8	依產業/類別而異。如：為《電信法》第222條訂定之「CPNI施行細則」規定，電信業者所分享資料之關係企業係為提供電信相關服務的業者以「選擇退出」模式，當資料主體欲撤回同意，即有權請求刪除其個人資料。	無相關法規	無相關法規

日本	個人情報 保護法	2003/5/30	●個人資料內容與事實不符 ●為超越特定利用目的為個人資訊之處理 ●以詐欺、其他不正當方法蒐集個人資料 ●未得到當事人同意將個人資料提供給第三人	●報導的事實性質及內容 ●事實傳達的範圍及隱私受害程度 ●當事人的社會地位及影響力 ●報導的目的及意義 ●社會的狀況 ●報導中公開當事人真實姓名及住址的必要性	刪除連結 不刪除原始資料
台灣	個人資料 保護法	2010/5/26	●違反個人資料保護法第 19 條(公務機關為第 15 條) ●特定目的消失或期限屆滿	無相關法規	無相關法規

資料來源：本研究自行整理

3.3.5 小結

我國學者認為，資料刪除權為隱私權之一部份，為憲法須保障之範圍，因此針對被遺忘權之修法建議方向為保障刪除權為基本方向，若有其餘考量必須限制刪除權的行使，須以明文訂定之方式，整體而言建議增加資料主體對資料的控制權(楊柏宏、陳銘雄，2016)。

3.4 分析結果引發偏誤與歧視

2016 年第三次的白皮書《Big Risks, Big Opportunities: the Intersection of Big Data and Civil Right》，其中大多為給予聯邦政府之建議，尤其大數據應用下應保護人民權利，避免人民受到歧視傷害。

大數據的應用亦可能加劇歧視問題(Dennis,2015; Woodcock,2016)，美國作家 Cathy O'Neil 的著作「Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy[76]」中提及原本社會存在的歧視可能導致他們表現的結果有所差異，但大數據分析僅會以結果論，因此結果可能顯示弱勢表現較差，更加劇了社會的歧視問題，亦可稱為「驗證偏誤」(Comfirmation bias)。例如美國過去以一「矯治服務量表」(Level of Service Inventory-Revised, LSI-R)評估犯人的再犯風險，當中的問題包含「過去親友是否曾被警察搜身的經驗？」、「第一次與警方交手的狀況如何？」，很明顯若調查對象本身身為容易受到歧視的弱勢族群，量表的指數就會相對偏高。可見大數據應用者容易將相關性與因果關係混淆，進一步加劇社會中的歧視。

除此之外，以徵才廣告為例，業者在網路上發送職缺廣告，就可能產生歧視行為。2015 年卡耐基梅隆大學的研究人員研發了名為 AdFisher 的工具，對其第三方網站上的廣告定向投放過程進行了追蹤。結果表明，當求職者為男性時，Google 將為其發送高新主管職缺資訊的機率相對於相同條件的女性求職者較高，但未必是男性能力較佳，可能是原先的社會狀況才導致了這種謬誤(香港矽谷，2016)。

我國學者葉志良亦於 2016 年指出大數據的發展下，由於各式資訊包含個人健康紀錄、位置資料等，更容易散佈於各地，隱私的保障愈加困難，且會產生歧視特定族群的問題。

3.4.1 美國於分析結果引發偏誤與歧視之看法

美國聯邦交易委員會於 1999 年於 In re Geocities 一案中，首度認定「業者違反其自身公布之隱私權保護政策，蒐集消費者個人資料」，意即構成聯邦交易委員法

[76] 台灣亦有作家許瑞宋將此著作翻譯為中文版，書名為「大數據的傲慢與偏見」。

第五條規定之「欺罔(deceptive)」行為。聯邦交易委員會更於 2005 年開始，多次以同法禁止「不公平(unfair)」行為之規範，擴大管制範圍，美國在處理關於大數據分析結果錯誤或歧視議題時，將授權於美國聯邦貿易委員會(Federal Trade Commission)判斷是否違反公平性，此法源於聯邦貿易委員法第五章，此法對於不公平行為加以規範，而構成不公平行為包含三大要件，「對消費者有潛在性傷害(Substantial Injury to Consumers)」、「無法合理性地避免(Not Reasonably Avoidable)」以及「傷害性超過益處(Outweighed by Countervailing Benefits)」，而美國聯邦貿易委員會認為業者利用大數據分析所造成之歧視性及錯誤性結果符合此一條件，因此將此一情形歸類為不公平之行為(Hirsch, 2015)。

2015 年 2 月，美國白宮發布「大數據與差別訂價(Big Data and Differential Pricing)」報告書，包含兩大部分。其一指出業者已開始利用大數據進行精準行銷及個人化定價，亦提到可以隱私法、反歧視法或消保法等方式解決。另外亦指出大數據之差別訂價使資訊不對稱問題更加嚴重，因此其中提到對於價格歧視的管制的建議。報告書內亦將此類行為分為「差別待遇(disparate treatment)」及「差別影響(disparate impact)」。「差別待遇」為業者以種族、性別、身分等消費者特徵作為較容易以反歧視法管制；但「差別影響」為大數據分析下，業者以特定族群不同類型的行為數據資料進行對消費者的負面影響，指表面上中立無歧視故意之措施，卻將造成特定族群之不利影響。因此「差別影響」於歐洲國家多稱之為「間接歧視(indirect discrimination)」，較難以以反歧視法管制。美國最高法院於 1971 年的 Griggs v. Duke Power Co.案例中，明確確立明美國民權法第 7 編同時禁止「差別待遇」及「差別影響」之就業歧視。但若為「差別影響」之情形，原告需提出證據以證明有差別影響之情形。被告若可證明其所採取之措施為合理如與「工作有關(job related)」、「業務需要(business necessity)」則可免責。但原告亦可提出具有「較小差別影響」之替代方案，以符合被告需求(黃昭元，2012)。

「從設計著手保護隱私」(Privacy by design)之概念亦漸漸受到學者重視(郭戎晉，2013; 蔡博坤，2013; 謝依彣，2014)，尤其大數據所帶來之新興隱私議題。FTC 除了呼籲各個私部門在設計階段即著手保護隱私(Privacy by design)，並同時推

動「禁止追蹤機制」(Do-Not-Track Mechnisms)，讓消費者可自行選擇是否留下數位足跡。

3.4.2 台灣於分析結果引發偏誤與歧視之看法

我國學者李進建亦在於中華民國律師公會全國律師期刊之文章「論大數據於犯罪偵查之挑戰與因應」指出，為符合反歧視法令要求，以大數據分析關聯性必須更加審慎，並且提到大數據的應用產生的歧視可能近一步導致勞工保護之問題。

另外，我國學者劉定基亦於《公平交易季刊》中，《欺罔與不公平資訊行為之規範－以美國聯邦交易委員會的管制案例為中心》一文中提到，不同於美國以授權聯邦交易委員會以行政管制之方式介入，我國目前並未授權任何相關機構處理此議題，僅在《個資法》中賦予該行業之「目的事業主管機關」行政監督及處罰權責，並非由專責的機關或單位辦理，成效相對不佳。

我國目前公平交易法第 20 條雖規定「無正當理由而給予差別待遇」之行為受禁止，但受保障之主體僅限於事業體，無法保障一般消費大眾。因此學者建議於消費者保護法第 24、25 條強化業者對於差別訂價之說明義務(王自雄，2016)。

大數據雖可能造成對特定族群的間接歧視，但相對地，亦可透過大數據之演算法協助對特定族群的保護。例如某一演算法所產生的訂價是否與種族產生正相關，可容易透過統計找出可能的「差別影響」。因此，學者認為可由主管機關適時進行相關影響評估(王自雄，2016)。

3.4.3 小結

美國俄亥俄州哥倫布法學院學者 Hirsch 於 2015 提及，美國目前訂定《公平合理信用報告法》，要求消費者徵信機構應當遵守的合理程序，規範分析內容不得有偏誤或具有歧視性內容，此類規範主要規範分析過程，避免資料主體因錯誤資訊或偏誤分析受到不合理對待，因此政府可針對大數據應用加強分析過程之規範。

為了建立公平的大數據應用原則，中國學者認為可明確訂定各領域之歧視性的利用，特定應用可被允許，如針對消費者偏好進行精準行銷；而限制特定潛在侵害人權或歧視之應用(李海英，2017)。此類方式與美國加強各類反歧視法有異曲同工

之妙。舉例來說，《信用機會平等法》(Equal Credit Opportunity Act)禁止信用供給者以性別、婚姻、種族、宗教或年齡等因素歧視或不平等對待信用交易申請人，《公平居住法》(Fair Housing Law)禁止任何房屋租售廣告包含任何基於種族、膚色、宗教、性別、身心障礙、家庭狀況或國族身份的偏好、限制或歧視。《民權法》(Civil Right Acts)也禁止在就業招聘廣告中涉及類似偏好、限制或歧視(Hirsch, 2015)。

中國大陸學者(张玉宏、秦志光、肖乐，2017)針對大數據歧視議題提出三大預防建議，包含增加大數據算法的透明性、以法律確保大數據算法的公平性以及從社會歧視問題事先預防。

3.5 大數據應用與我國現行隱私法之衝突與可行做法

本研究除個別說明各國於上述四大議題之現況及看法之外，並將上述大數據應用四大議題，與我國現行法規之衝突彙整於下<表 3-5>。「資料蒐集告知困境」主要為以選擇加入或選擇退出模式之爭議，「去識別化與在識別化風險」主要與間接識別與去識別之定義。「刪除權行使的限制或擴張」本研究將分為非公開個人資料及公開個人資料，非公開資料如消費者提供給業者之個人資料等第三方無法任意取得之資料；公開資料如搜尋引擎可搜尋之新聞等公眾可取得之個人資料。「分析結果引發偏誤與歧視」主要問題則為台灣目前無針對此議題之相關規範。

表 3-5 大數據應用下議題與我國現行法規之衝突

議題	我國現行相關法規	與大數據應用之衝突
資料蒐集告知困境	個資法第 15 條及 19 條，公務及非公務機關對個人資料之蒐集或處理須告知資料主體且取得同意。 個資法第 8 條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：	若法規以「選擇加入」模式為主，則會加重業者大數應用蒐集告知成本(Tene & Polonetsk, 2012)。反之若法規以「選擇退出」模式，對資料主體之保護有限，因一般消費者可能對隱私權政

	一、公務機關或非公務機關名稱。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、對象及方式。 五、當事人依第三條規定得行使之權利及方式。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。	策或服務條款不甚了解，存在資訊不對稱獲知識落差問題(翁清坤，2013)。而目前我國以選擇加入為主，選擇退出為例外，對大數據應用為一大限制。
去識別化與再識別風險	個資法第 3 條規定，間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。	去識別化標準不明確，台灣並無法定標準，僅有較嚴格之國家標準，但不具強制性，以「一般人基準說」為判斷依據，「其他資訊」應限於已公開、被公知資訊，以作組合、比對之可能，但事實並非如此(王慕民等，2015)。
刪除權行使的限制或擴張	個資法第 11 條規定，個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。	四、非公開個人資料： 大數據應用需蒐集大量數據才可達最佳效果，限縮刪除權與否成為重要癥結點。 五、公開個人資料：

	個資法第 9 條規定，蒐集非當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及機構名稱。	由於個資法第 9 條將當事人自行公開或已合法公開之個人資料轉載列為不須告知資料主體之情況，當事人無法請求轉載之第三方刪除內容或連結。因此目前我國之被遺忘權尚未確立。
分析結果引發偏誤與歧視	目前台灣無規範大數據應用過程避免結果偏誤及歧視之相關法律，僅有既有部分反歧視法。	目前有部分國家針對大數據應用可能引發偏誤與歧視問題訂定法律規範，如美國以《公平合理信用報告法》規範信用報告機構分析過程必須合理，並以《信用機會平等法》、《公平居住法》、《公平機會法》（Fair Chance Act)等反歧視法防止歧視問題。然而目前台灣無規範大數據應用過程避免結果偏誤及歧視之相關法律。

資料來源：本研究整理

綜觀上述各個大數據世代之議題，本研究已彙整各國相關規範、發展以及學者之相關建議。本研究將於此節彙整各個議題下，可能之改善方向分述如下，而選擇其作法之原因如下<表 3-6>。

表 3-6 本研究選擇各個作法之原因

資料蒐集 告知困境作法	資料蒐集機制分為**選擇加入**及**選擇退出**機制(翁清坤，2013)	1.選擇加入(opt-in)	如歐盟與台灣現行做法。(Milne, 2000; 翁清坤，2013; Sakshaug et al., 2016)
		2.選擇退出(opt-out)	如美國與歐盟於 2000 年訂定協議之《安全港協議》[77](Safe Harbor Agreement)之資料蒐集機制(Weiss & Archic, 2016)。
	3.以部門式立法，依照產業需求。		美國現行做法。如《電信法》要求電信業者所分享的關係企業係為提供電信相關服務的業者，其同意模式乃採「選擇退出」方式；而分享至第三方或其他非關係企業包含合夥投資人、獨立包商等，皆須以「選擇加入」機制為基礎(翁清坤，2017)。
	4.以事後管制代替事前管制。		美國總統科學和技術顧問委員會(President's Council of Advisors on Science and Technology,PCAST)以及 Mayer-Schönberger and Cukier (2013)則是主張以「事後管制」取代「事前管制」。業者雖可自由蒐集消費者之個人資料，但業者將保證資料的利用將不會對資料主體造成任何侵

[77] 參照本文 2.4.2。一般個人資料以「選擇退出」(opt-out)為主，敏感性資料則採用選擇加入機制。

		害，若造成任何隱私侵害將由業者負擔相關賠償以及法律責任(吳珞齊，2017; 彭金隆等，2017)。
去識別化與再識別風險作法	1.訂定「去識別化」檢驗標準，依照標準進行個案判定，且「**須**」將原始資料(庫)一併刪除。	參考歐盟現行做法(歐盟第 29 條工作小組 2014 年之意見書 0829/14/EN WP216)。
	2.訂定「去識別化」檢驗標準，依照標準進行個案判定，但「**不須**」將原始資料(庫)一併刪除。	
	3.訂定去識別化的「安全港準則」，列出必須刪除之個資項目，刪除後即符合去識別化標準；若有特例需求，則再輔以專家判斷評估風險。	美國去識別化標準為《醫療保健及責任法案》 (Health Insurance Portability and Accountability Act) 最具代表性(蔡昀臻、樊國楨，2016; Garfinkel, 2015)。
	4.針對去識別技術加以限制，規定須以包含加入干擾之方式為之，如「雜訊加入」、「差分隱私」等。故一般以遮蔽個人資料的方式，如「資料代碼化處理」、「取代」等方式，則不符合去識別化之標準。	學者建議(Narayanan, A., Huey, J., & Felten, E. W. ,2016)。

被遺忘權	鼓勵刪除權擴張，行使被遺忘權。	歐盟現行做法，法規(GDPR)明定之人民權利。
	鼓勵刪除權擴張，但從嚴行使被遺忘權。	日本現行做法，雖無明確法規，但東京法院公布被遺忘權之標準。
	限制刪除權擴張，不行使被遺忘權。	由於美國憲法第一條增修條文，保障商業自由，因此採取此作法。

對於「資料蒐集告知困境」之議題，本研究共彙整四種作法，分述如下：

一、作法 1

對於資料蒐集的告知，歐盟與台灣的法律皆**以「選擇加入」為主，亦即個人資料的蒐集與利用，必須告知當事人之後，方可進行。**

二、作法 2

為解決現行個資法要求告知義務之困境，有學者認為**可將有利經濟發展之大數據應用排除現行個資法規範之外，如增修個資法第 51 條豁免適用範圍，或增修個資法第 8 條蒐集告知義務，增加豁免適用範圍。**

三、作法 3

美國則是以「部門式」立法，將蒐集資料之告知義務各別納入各產業相關法規中。若欲參照美國法，則可**訂定產業特別法，並於其中排除個資法告知義務。**

四、作法 4

另有學者 (Mayer-Schönberger and Cukier, 2013)主張**以「事後管制」取代「事前管制」，開放業者可自由蒐集消費者個人資料而不須事前告知，但對於業者及資料使用者則課以隱私保護之義務，若消費者(資料主體)受到隱私侵害，則可請求損害賠償**。

對於「去識別化與再識別風險」之議題，本研究彙整四種作法，分述如下：

一、作法 1

對於「去識別化與再識別風險」，歐盟目前做法為，**訂定『去識別化』檢驗標準**(主要檢驗『去識別化』後，是否仍可能識別資料主體、是否可與其他資料相連、

是否仍可推論出特定人相關)」，**依照個案判定是否達到此標準，並要求將原始資料一併刪除。**

二、作法 2

參照歐盟目前作法，**訂定「去識別化」檢驗標準，依照標準進行個案判定，但「不須」將原始資料(庫)一併刪除。**

三、作法 3

美國『去識別化』的檢驗方式為**訂定「安全港準則」，列出必須刪除的個資項目，(例如：姓名、帳戶號碼、電話號碼等)，刪除後即符合『去識別化』標準**；然而若有特例，或須進一步檢驗，則再**輔以「專家判斷評估風險」**，決定是否達到去識別化標準。

四、作法 4

亦有學者認為『去識別化』標準，可考慮**針對去識別技術加以限制，須以特定技術為之，例如加入特定干擾技術(「雜訊加入」、「差分隱私」等)，藉此以達去識別效果**。反之，一般以遮蔽個人資料的方式，例如「資料代碼化處理(Pseudonymisation) (Token)」、「取代(Substitution)」等方式，則因未加入特定干擾技術，故不符合去識別化之標準。

對於「刪除權行使的限制或擴張」之議題，本研究彙整三種作法，分述如下：

一、作法 1

鼓勵刪除權擴張，行使被遺忘權。對於刪除權行使的限制或擴張，歐盟目前於個資法規範內**明確賦予資料主體對於個人資料相關『連結』的刪除權(亦稱作「被遺忘權」)。凡是內容已無存在必要，且與公共利益無關，資料主體則可對搜尋引擎行使刪除權(被遺忘權)。**

二、作法 2

鼓勵刪除權擴張，但從嚴行使被遺忘權。日本對於刪除權之擴張採從嚴辦理，例如根據 2017 年東京法院判決提出，須**以特定檢驗標準判定刪除權擴張與否 (如資料主體是否為公眾人物、內容侵害隱私程度等)，唯有保護隱私權的價值明顯高於資訊公開才得以行使被遺忘權。**

三、作法 3

亦有學者認為應參照美國**維護言論自由及資訊流通，主張維持現狀不提供資料主體刪除已公開個人資料之權利。**

對於「分析結果引發偏誤或歧視」之議題，本研究彙整兩種做法，分述如下：

一、作法 1

參照美國訂定《公平合理信用報告法》，**要求提供消費者報告之業者遵守的合理程序，針對大數據應用加強分析過程之規範。**

二、作法 2

公平交易法第 20 條限制競爭部分「無正當理由而給予差別待遇」保障之主體僅限事業體，可進一步修增公平交易法，保障一般消費大眾。並授權公平交易委員會或其他專責機構以行政管制之方式，將其視為「不公平行為」，監督及處罰違規之業者。

三、作法 3

參照歐盟 GDPR 拒絕權與個人化自動決策規範，授予資料主體拒絕自動化處理且對其產生法律效果或重大影響之決策之權利，但若為締結或履行資料主體與資料控制者間之契約，或有獲得資料主體明確同意書，則不在此限。

本研究將於第下一章實證研究，將所彙整之作法用以建構 AHP 層級架構，近一步分析各關鍵隱私議題相對權重以及改善作法之相對權重。

第四章 實證研究

透過文獻回顧及比較研究，本研究已彙整各個大數據關鍵隱私議題並比較各國相關現況及作法。本研究將進一步進行實證研究，包含修正式德爾菲法及 AHP 層級分析法。透過修正式德爾菲法加以證實各個關鍵議題是否為專家所認同之大數據世代關鍵隱私議題。並透過 AHP 層級分析法進行各關鍵議題下專家對各個改善方案之重要性權重分析。

4.1 修正式德爾菲法

修正式德爾菲法為 Murry 與 Hammoms 於 1995 年所提出，主要流程須先以文獻回顧方式蒐集相關議題，再進一步透過層級分析法確定研究主題。詳見 1.4 研究方法。

4.1.1 文獻回顧

本研究以修正式德爾菲法建立 AHP 層級架構，層級架構之主要目標為為大數據應用所面臨之隱私議題，本研究透過修正式德爾菲法初步從文獻等資料，分析大數據世代下隱私議題，作為探討之基礎，如<表 4-1>所示。

表 4-1 修正式德爾菲法議題文獻回顧

目標	大數據應用下之隱私議題	參考文獻
改善大數據應用下我國現行隱私之保護	去識別化與再識別風險	Sweeney(2000)、Ohm(2010)、United States. Executive Office of the President, & Podesta, J. (2014)、Garfinkel(2015)、Narayanan, et al.(2016)
	刪除權行使的限制或擴張	Ohm(2011)、Weber(2011)、Tene & Polonetsky(2012)、Rosen(2012)、Mantelero(2013)、 United States. Executive Office of the President, & Podesta, J. (2014)
	分析結果引發偏誤與歧視	United States. Executive Office of the President, & Podesta, J. (2014)、Dennis(2015)、Woodcock(2016)、香港矽谷(2016)、葉志良(2016) 、Munoz, C., Smith, M., & Patil, D.(2016)
	資料蒐集的告知困境	Tene & Polonetsk(2012)、Jensen(2013)、Tung(2013)、Kshetri(2014)、United States. Executive Office of the President, & Podesta, J. (2015)

資料來源：本研究整理

4.1.2 問卷設計與專家選擇

為了能利用 AHP 層級分析法找出改善大數據應用下我國現行隱私之保護方向，本研究先利用修正式德爾菲法篩選出大數據應用下之隱私議題，本研究採用李克特五點量表尺度作為衡量工具。Wheeller et al. (1990) 建議修正式德爾非法 10-12 人或 15-20 人為宜，因此本研究問卷填答專家係由八位產業界大數據分析之專家及三位學術界相關領域之專家所進行，其專家名單如表<4-2>所示。專家問卷發放時間為 2017 年 7 月 21 日至 2017 年 8 月 5 日。透過 Google 表單，以電子郵件方式進行發放。

表 4-2 修正式德爾菲法專家選擇

類別	服務單位	職稱	姓名	專業領域
Professors	國立成功大學交通管理科學系電信管理研究所	助理教授	黃光渠	網路安全、電信政策
	元智大學資訊傳播學系	助理教授	葉志良	資通訊法律、智慧財產權
	國立高雄科技大學科技法律研究所	教授	程法彰	智慧財產權、隱私、通訊
Industry experts	玉山銀行	數位行銷專員	劉凱翔	數位行銷
	玉山銀行	數據分析專員	孫書恩	大數據分析
	藍科數位科技-台灣銀行	資料分析工程師	林昭宏	資料科學
	聯合通商-遠傳電信	系統設計師	陳敏勝	資料倉儲
	中華電信	工程師	王薔惠	大數據分析
	中華電信	協理	鍾國強	電信技術與法規
	遠傳電信	協理	蕭景騰	電信法規政策、通訊傳播產業分析
	台灣大哥大	處長	吳中志	通訊傳播法規政策、網路互連

資料來源：本研究整理

4.1.3 問卷統計結果

由<表 4-3>所示，在次要層級「大數據應用下之隱私議題」構面中，專家認為「去識別化與再識別風險」最具有大數據應用下隱私議題之代表性及重要性(平均得分為 4.4 分)，「資料蒐集的告知困境」次之(4.3 分)，而「分析結果引發偏誤與歧視」最不具代表性及重要性(3.6 分)。由於「分析結果引發偏誤與歧視」平均得分低於 4 分，因此本研究將不採用此議題以建立 AHP 層級架構。由於 Holden & Wedman(1993)提出當問卷之題項 70%達到一致性或穩定時，則問卷施測即可停止，本次問卷結果之標準差皆≦1、變異係數皆小於 50%(Hsu & Chen, 2007)且眾數與平均數之差的絕對值皆≦1(郭聰明、林利國、張凱銘，2015)，上述結果皆表示專家意見一致性趨於穩定，因此本研究不繼續第二回合之問卷。

表 4-3 修正式德爾菲法議題篩選結果

大數據應用下之隱私議題	平均得分	變異係數	眾數	|眾數－平均數|	評選結果
資料蒐集的告知困境	4.3	11.02%	4	0.3	採用
去識別化與再識別風險	4.4	11.18%	4	0.4	採用
刪除權行使的限制或擴張	4.0	26.11%	5	1	採用
分析結果引發偏誤與歧視	3.6	29.36%	4	0.4	不採用

資料來源：本研究整理

4.1.4 小結

本研究之修正式德爾菲法平均分數皆偏高，表示專家對於文獻回顧之四大議題皆相當重視，相關議題研究紛紛出籠，可見大數據世代下關鍵隱私議題已漸漸浮現於檯面。不僅 2014 年至 2016 年美國逐年發布之三次《大數據白皮書》(United States. Executive Office of the President, & Podesta, J., 2014; United States. Executive Office of the President, & Podesta, J., 2015; Munoz, C., Smith, M., & Patil, D., 2016)，亦已有不少文獻針對各別議題進行相關研究[78]，因此本研究採用相對較高標準平均 4

[78] 參閱表<4-1>。

分以上為篩選標準，故通過篩選之三大議題應能有效代表專家所認同之大數據關鍵隱私議題。

「分析結果引發偏誤與歧視」議題，國外研究如美國已有諸多文獻，但本研究結果顯示，本研究之修正式德爾菲法分析結果中，此議題未達採用標準。雖然此議題並未達到採用標準，但其變異係數較高，可見專家意見相對一致性較低。部分專家認為雖認同此為重要議題，但認為其與隱私相關性較低，因此給予低分。除此之外，本研究推斷可能原因尚有二。第一，專家對於資料較具有高度敏感度，且受侵害之資料主體多屬社會基層或弱勢族群。第二，以相關文獻而言，我國對於此議題之重視度尚屬偏低，且大部分未意識到大數據分析結果僅為相關性，不等於因果關係，進而忽略此議題。本研究認為此議題可能尚屬大數據關鍵隱私議題，建議後續研究亦可針對此議題進行深入探討。

雖問卷結果之各項「變異係數」及「眾數與平均之差的絕對值」皆符合學者所建議之標準，表示專家意見一致性趨於穩定，但四大議題中，「刪除權行使的限制或擴張」及「分析結果引發偏誤與歧視」之變異係數及「變異係數」及「眾數與平均之差的絕對值」較高，代表專家對於此兩議題之一致性較低，意見相對極端，部分專家對於將此兩議題歸納為大數據世代下隱私關鍵議題之認同度較低。

4.2 AHP 層級分析法

過去許多研究結合德爾菲法與層級分析法作為主要研究方法，舉凡業者之決策至政府政策訂定，如供應商的選擇(Liao, 2010; Raut, 2014)、保險方案的訂定(Huang, 2008)、國家的進出口政策(Kim, 2012)等。2011 年 Vidal 等學者以德爾菲法為發展基礎之層級分析法之文獻，說明此研究方法如何用以評估複雜決策，即是重要代表之一。本研究將透過 AHP 層級分析法進行各關鍵議題下專家對各個改善方案之重要性權重分析。

4.2.1 AHP 層級分析法介紹

應用層級分析法處理複雜議題時，需事先進行問題描述，進一步找出影響要素，並建立層級關係、採用成對比較的方式評估各層級要素之相對重要性，我國學者曾國雄、鄧振源(1989)以 Saaty(1980)所提出層級分析法為基礎，進一步介紹內涵特性以及應用，大致可分為下述幾大步驟：

一、問題的界定及找出影響因素

決定問題的主要目標，對於問題所應盡量擴大影響問題的因素，將之皆納入問題中。

二、建立 AHP 層級結構

處理主題較為複雜之問題時，利用層級結構加以分解，因此須找出主要目標的各項指標或評估準則，或是列入各個替代方案。但由於人類難以對七種以上事物同時進行比較，因此每一層之要素不宜超過七個。

三、問卷設計與調查

完成建立層級結構後之步驟後，進行問卷調查，讓受訪者透過兩兩準則之間相對重要性，Saaty(1980)建議尺度於 1 至 9 尺度進行設計，劃分為絕對重要、極重要、頗為重要、稍微重要及同等重要問卷須包含詳細引導說明。

四、建立成對比較矩陣

根據問卷調查所得到的兩兩相比結果，建立各層級之成對比較矩陣 A。分別以 1/9，1/8，...，1，2，3，...，8，9 為成對比較之數值，將 n 個要素比較結果的衡量，置於成對比較矩陣 A 的上三角形部分，而下三角形部分相對位置數值的倒數，即 aji＝1/aij，其元素之成對比較矩陣如下所示：

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}=\begin{bmatrix} w_1/w_1 & w_1/w_2 & \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \cdots & w_2/w_n \\ \vdots & \vdots & \cdots & \vdots \\ w_n/w_1 & w_n/w_2 & \cdots & w_n/w_n \end{bmatrix}$$

五、計算特徵值與特徵向量，求各層級要素間相對權重

將取得之成對比較矩陣 A，採用特徵向量的理論基礎，用以計算出特徵向量與特徵值，進而求得各要素，於本研究即為議題或改善方案之間的相對權重。計算過程說明如下：

步驟一：

建立準則成對比較矩陣 A，如(1)式

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}=\begin{bmatrix} w_1/w_1 & w_1/w_2 & \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \cdots & w_2/w_n \\ \vdots & \vdots & \cdots & \vdots \\ w_n/w_1 & w_n/w_2 & \cdots & w_n/w_n \end{bmatrix} \quad (1)$$

其中 $a_{ij}=w_i/w_j$ ， w_i, w_j 各為準則 i 與 j 之權重

準則成對比較矩陣 A 為一正倒值矩陣，符合矩陣中各要素為正數，且具倒數特性，如(2)式與(3)式：

$$a_{ij}=1/a_{ji} \quad (2)$$

$$a_{ij}=a_{ik}/a_{jk} \quad (3)$$

步驟二：

將準則成對比較矩陣 A 乘上各準則權重所成之向量 $\overline{w}$ ：

$$\overline{w}=\left(w_1, w_2, \cdots, w_n\right)^t \quad (4)$$

可得(5)式與(6)式：

$$A\overline{w}=\begin{bmatrix} w_1/w_1 & w_1/w_2 & \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \cdots & w_2/w_n \\ \vdots & \vdots & \cdots & \vdots \\ w_n/w_1 & w_n/w_2 & \cdots & w_n/w_n \end{bmatrix}.\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \quad (5)$$

$$A\overline{w}=n\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \quad (6)$$

亦即 $(A-nI)\overline{w}=0$ (7)

因為 aij 乃為決策者進行成對比較時主觀判斷所給予的評比，與真實的 wi/wj 值，必有某程度的差異，故 $A\overline{w}=n\overline{w}$ 便無法成立，因此，Saaty 建議以 A 矩陣中最大特徵值 λmax 來取代 n。

亦即 $A\overline{w}=\lambda_{\max}\overline{w}$ (8)

$(A-\lambda maxI)\ \overline{w}=0$ (9)

矩陣 A 的最大特徵值之求法，由 (9)式求算出來，所得之最大特徵向量，即為各準則之權重。而最大特徵值之求算，Saaty 提出四種近似法求取，其中又以行向量平均值的標準化方式(10)式可求得較精確之結果。

$$w_i=\frac{1}{n}\sum_{j}^{n}\frac{a_{ij}}{\sum_{i=1}^{n}a_{ij}} \qquad i,j=1,2,\cdots,n \quad (10)$$

六、一致性檢定

在此理論之基礎假設上，假設 A 為符合一致性的矩陣，但是由於填卷者主觀之判斷，使其矩陣 A 可能不符合一致性，但評估的結果要能通過一致性檢定，方能顯示填卷者的判斷前後一致，否則視為無效的問卷。因此 Saaty 建議以一致性指標(Consistence Index,C.I.)與一致性比例(Consistence Ratio,C.R.)來檢定成對比較矩陣的一致性。

- 一致性指標(C.I.)

一致性指標由特徵向量法中求得之λ_{max}與 n(矩陣維數)兩者的差異程度可作為判斷一致性程度高低的衡量基準。

$$C.I. = \frac{\lambda_{max} - n}{n-1} \qquad (11)$$

當 C.I. =0 表示前後判斷完全具一致性，而 C.I. >0 則表示前後判斷不一致。Saaty 認為 C.I. < 0.1 為可容許的偏誤。

- 一致性比例(C.R.)

根據 Oak Ridge National Laboratory & Wharton School 進行的研究，從評估尺度 1-9 所產生的正倒值矩陣，在不同的階數下所產生的一致性指標稱為隨機性指標 (Random Index; R.I.)，見下表<4-1>。

在相同階數的矩陣下 C.I.值與 R.I.值的比率，稱為一致性比率 C.R. (Consistency Ratio) 即：

$$C.R. = \frac{C.I.}{R.I.} \qquad (12)$$

若 C.R.< 0.1 時，則矩陣的一致性程度使人滿意。

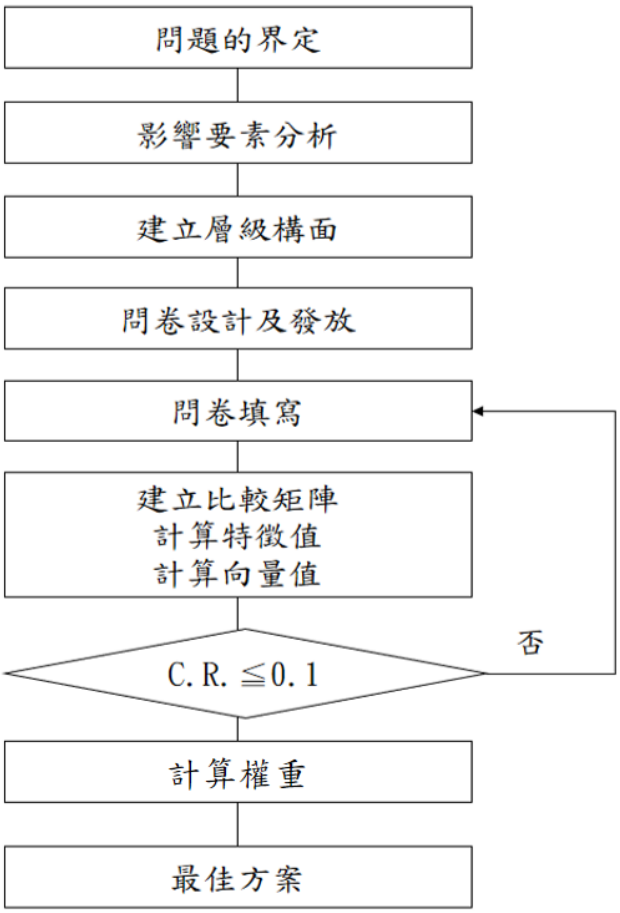
表 4-4 AHP 隨機指標表

階數	1	2	3	4	5	6	7	8
R.I.	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41
階數	9	10	11	12	13	14	15	-
R.I.	1.45	1.49	1.51	1.48	1.56	1.57	1.58	-

資料來源：曾國雄、鄧振源(1989)

層級分析法流程如下<圖 4-1>所示：

圖 4-1 AHP 層級分析法流程圖



資料來源：曾國雄、鄧振源(1989)

4.2.2 建立 AHP 層級架構

本研究之目標為大數據世代下改善我國現行隱私保護方向選擇，為了達到此一目標，本研究透過第三章彙整之四大議題，加以透過修正式德爾菲法，進一步篩選為三大關鍵隱私議題。除此之外，本研究亦個別彙整各議題之各國改善作法或者學者建議改善作法，用以建構 AHP 層級架構。層級分析架構彙整如下<圖 4-2>所示。

圖 4-2 本研究層級分析(AHP)之架構圖

參考資料：本研究整理

4.2.3 研究設計與專家選擇

本研究以上述層級架構圖，將各個層級內的要素以兩兩比對的比較方式設計 AHP 專家問卷。可將問卷內容分為兩大部分，其一為主要層級，主要評估主要構面，即為各個議題間之相對重要性。第二為主要構面下的要素，即為議題之改善方案間的相對重要性。

本研究根據 AHP 準則將評估尺度劃分為 1-9 項衡量值，評估尺度可分為五個不同基本等級，分別為同等重要、稍重要、頗重要、極重要以及絕對重要。為了量化評估，分別以 1、3、5、7、9 代表，另有 2、4、6、8，此四衡量值介於五個基本等級之間，關於各尺度所代表之涵義如表<4-4>。

表 4-5 AHP 評估尺度

評估尺度	定義	說明
1	同等重要(Equal Importance)	兩比較方案的貢獻度具同等重要。 等強(Equal)

3	稍重要(Weak Importance)	經驗與判斷稍微傾向喜好某一方案。稍強(Moderately)
5	頗重要(Essential Importance)	經驗與判斷強烈傾向某一方案。頗強(Strongly)
7	極重要(Very Strong Importance)	實際顯示非常強烈傾向喜好某一方案。極強(Very strongly)
9	絕對重要(Absolute Importance)	有足夠證據肯定絕對喜好某一方案。絕強(Extremely)
2、4、6、8	相鄰尺度的中間值(Intermediate Value)	需要折衷值時

參考資料：曾國雄、鄧振源(1989)

本研究的目的主要在找出大數據世代下關鍵隱私議題的改善方向，試圖從各主要構面議題下的做法找出最合適我國的改善方向，並提供建議專家名單如表<4-6>，。本此研究因涉及大數據相關應用、個人資料及隱私相關法律的制定與規範，為了讓本研究的結果更能代表業界又不過於偏頗，主要選擇考量如下：

一、本研究考量研究的對象必須對大數據相關應用有基本了解，再專家的選擇方面涵蓋了大數據相關應用或分析之業者、通訊傳播法規政策或隱私權、個資法、網路安全相關之專家。

二、財團法人資訊工業策進會及亞太網路資訊中心之專家。財團法人電信技術中心為我國資通訊傳播政策重要機構，大數據應用及隱私保護為資通訊傳播政策相關議題。財團法人資訊工業策進會為政府經濟部為推動資訊科技發展而成立支機構，為我國訂定資訊政策及法律重要研究機構。亞太網路資訊中心，全球五大區域性網際網路註冊管理機構之一，涉及網路安全問題。綜觀上述，本研究邀請此三大研究機構之專家填寫專家問卷。

三、電信業及金融業皆為個人資料蒐集及數據分析最為廣泛之產業之一，因此本研究邀請四位電信業專家及四位金融業專家填寫問卷。除此之外，本研究尚邀請資訊科技產業兩人及法律界專家一人以期獲得更多元之看法。

四、本次問卷對象包含學術專家 3 人、研究專家 7 人、業界專家 10 人，共 20 人。三位學術專家專業領域皆涉及資訊隱私，同時為資訊及隱私相關專業。八位研究專家包含財團法人電信技術中心、財團法人資訊工業策進會及亞太網路資訊中心之專家。

表 4-6 AHP 專家問卷訪談對象

類別	服務單位	職稱	姓名	專業領域
學(研)界專家	國立成功大學交通管理科學系電信管理研究所	助理教授	黃光渠	網路安全、電信政策
	元智大學資訊傳播學系	助理教授	葉志良	資通訊法律、智慧財產權
	國立高雄科技大學科技法律研究所	副教授兼所長	程法彰	智慧財產權、隱私權、通訊
	亞太網路資訊中心	董事暨準執行長	黃勝雄	通訊網路、網路治理、公司治理、網路安全
	財團法人電信技術中心	副研究員	王牧寰	電信法、數位媒體法、數位匯流政策、能源資通訊政策
	財團法人電信技術中心	研究企劃組主任	陳人傑	通訊傳播政策及法律
	財團法人電信技術中心	專案經理	陳志宇	數位匯流法制、通訊傳播法制、無線電頻譜管理政策、資通訊安全政策
	財團法人電信技術中心	數位匯流專案辦公室組長	黃志雯	通訊傳播、新媒體
	財團法人資訊工業策進會	科技法律研究所副所長	孫文玲	科技法律
	財團法人資訊工業策進會	科技法律研究所科技應用法治中心副主任兼應研組組長	郭戎晉	個人資料保護、隱私保護

	財團法人中華民國國家資訊基本建設產業發展協進會	執行長	陳文生	資訊管理、資訊安全、網路治理
業界專家	台灣大哥大	法規暨同業關係處處長	吳中志	通訊傳播法規政策、網路互連
	中華電信	法律事務處協理	鐘國強	電信技術與法規
	遠傳電信	電信公司法規部協理	蕭景騰	電信法規政策、通訊傳播產業分析
	理律法律事務所	資深律師	簡維克	公平交易法、通訊傳播、個人隱私
	玉山銀行	數位行銷專員	劉凱翔	數位行銷
	玉山銀行	數位行銷資深專員	孫書恩	數位行銷
	碩益科技	商業智慧顧問	廖棋弘	資料分析
	藍科數位科技-台灣銀行	資料分析工程師	林昭宏	資料科學
	聯合通商-遠傳電信	系統設計師	陳敏勝	資料倉儲

4.3 AHP 層級分析法分析結果

本章節透過 AHP 層級分析法之統計分析軟體 Expert Choice 2000 進行問卷分析，首先建立成對矩陣，進一步分析各構面下之權重，最後藉由一致性檢定檢驗分析結果是否合理。本研究將依序進行權重分析，首先將針對關鍵隱私議題構面分析，進而依序探討三大隱私議題改善作法之相對權重分析，包括資料蒐集告知困境、去識別化與再識別風險以及刪除權行使的限制或擴張進行權重分析，進行相對重要性之優先順序排序。

4.3.1 問卷處理

本研究從資料蒐集告知困境、去識別化與再識別風險以及刪除權行使的限制或擴張三大關鍵隱私題三個構面以改善大數據世代下我國現行隱私保護法，並提出建議。問卷一般以親自訪問或電子郵件方式發放，本研究問卷以電子郵件方式發放，並於信件內補充說明須注意一致性之問題。依 4.2.4 節之專家選擇考量，首先發出 20 份問卷，回收 19 份，有效問卷總共 19 份，包含學術專家 3 人、研究專家 7 人業界專家 9 人。專家問卷發放時間為 2017 年 11 月 16 日至 2017 年 12 月 25 日。

4.3.2 關鍵隱私議題相對權重分析

關鍵隱私議題構面相對權重評估包含資料蒐集告知困境、去識別化與再識別風險、刪除權行使的限制或擴張。如表<4-7>，在衡量議題構面層級的權重分析中，資料蒐集告知困境相對權重佔 41.3%，去識別化與再識別風險權重值佔 42.4%，刪除權行使的限制或擴張權重值佔 16.3%，C.R.≦0.1 表示此分析結果符合一致性檢驗標準。整體構面的相對權重如<表 5-1>所示，結果顯示，在議題構面層級中資料蒐集告知困境是整體專家最重視的構面，其次為去識別化與再識別風險，最後為刪除權行使的限制或擴張。

表 4-7 大數據世代下關鍵隱私議題相對權重排序

構面	權重	排序
資料蒐集告知困境	0.413	2
去識別化與再識別風險	0.424	1
刪除權行使的限制或擴張	0.163	3
C.R.	0.010	
C.I.	0.006	
R.I	0.580	

資料來源：本研究　　整理

註：(1)C.R. (Consistency Ratio)，一致性比例， $C.R. = \frac{C.I.}{R.I.}$ *。*

(2)C.I. (Consistence Index)，一致性指標， $C.I. = \frac{\lambda_{max} - n}{n-1}$ *，其中* $\lambda_{\max}$ *為矩陣 A 的最大特徵值。*

(3)R.I. (Random Index)，隨機性指標，正倒值矩陣，在不同的階數下所產生的一致性指標。

4.3.3 資料蒐集告知困境相對權重分析

資料蒐集告知困境議題中，需評估權重的作法包含以下：

一、嚴格執行告知義務，維持現狀採取「選擇加入」模式，要求業者蒐集資料前須告知消費者(以下簡稱：嚴格執行告知義務)。

二、修改現行個資法，以修法方式，將有利於經濟發展之大數據應用排除個資法規範之外(以下簡稱：於現行個資法中增訂豁免規定)。

三、以「部門式」立法，訂定產業特別法，排除個資法告知義務適用範圍(以下簡稱：以部門式立法排除告知適用)。

四、以「事後管理」取代「事前管理」，開放業者自由蒐集消費者個人資料，但對於資料使用者課以保護資料主體隱私權之義務(以下簡稱：以事後管理取代事前管理)。

根據統計軟體分析結果，如表<4-8>，「嚴格執行告知義務」相對權重值佔27.6%，「於現行個資法中增訂豁免規定」相對權重值佔23.2%，「以部門式立法排除告知適用」相對權重值佔31.3%，而「以事後管理取代事前管理」相對權重值佔18%。

表 4-8 資料蒐集告知困境改善作法相對權重排序

構面	權重	排序
嚴格執行告知義務，維持現狀採取「選擇加入」模式，要求業者蒐集資料前須告知消費者。	0.276	2
修改現行個資法，以修法方式，將有利於經濟發展之大數據應用排除個資法規範之外(於現行個資法中增訂豁免規定)。	0.232	3
以「部門式」立法，訂定產業特別法，排除個資法告知義務適用範圍。	0.313	1
以「事後管理」取代「事前管理」，開放業者自由蒐集消費者個人資料，但對於資料使用者課以保護資料主體隱私權之義務。	0.180	4
C.R.	0.000	
C.I.	0.000	
R.I	0.9	

資料來源：本研究整理

4.3.4 去識別化與再識別風險相對權重分析

去識別化與再識別風險議題中，需評估權重的作法包含以下：

一、訂定「去識別化」檢驗標準，依照標準進行個案判定，且「**須**」將原始資料(庫)一併刪除(以下簡稱：訂定檢驗標準並要求刪除原始資料)。

二、訂定「去識別化」檢驗標準，依照標準進行個案判定，但「**不須**」將原始資料(庫)一併刪除(以下簡稱：訂定檢驗標準但不要求刪除原始資料)。

三、訂定去識別化的「安全港準則」，列出必須刪除之個資項目，刪除後即符合去識別化標準；若有特例需求，則再輔以專家判斷評估風險(以下簡稱：訂定去識別化之安全港準則)。

四、針對去識別技術加以限制，規定須以包含加入干擾之方式為之，如「雜訊加入」、「差分隱私」等。故一般以遮蔽個人資料的方式，如「資料代碼化處理」、「取代」等方式，則不符合去識別化之標準(以下簡稱：以技術規範加以限制)。

表 4-9 去識別化與再識別風險改善作法相對權重排序

構面	權重	排序
訂定「去識別化」檢驗標準，依照標準進行個案判定，且「**須**」將原始資料(庫)一併刪除。	0.231	3
訂定「去識別化」檢驗標準，依照標準進行個案判定，但「**不須**」將原始資料(庫)一併刪除。	0.179	4
訂定去識別化的「安全港準則」，列出必須刪除之個資項目，刪除後即符合去識別化標準；若有特例需求，則再輔以專家判斷評估風險。	0.266	2
針對去識別技術加以限制，規定須以包含加入干擾之方式為之，如「雜訊加入」、「差分隱私」等。故一般以遮蔽個人資料的方式，如「資料代碼化處理」、「取代」等方式，則不符合去識別化之標準。	0.324	1
C.R.	0.002	
C.I.	0.002	
R.I	0.9	

資料來源：本研究整理

根據統計軟體分析結果，如<表 4-9>，「訂定檢驗標準並要求刪除原始資料」相對權重值佔 23.1%，「訂定檢驗標準但不要求刪除原始資料」相對權重值佔 17.9%，「訂定去識別化之安全港準則」相對權重值佔 26.6%，而「以技術規範加以限制」相對權重值佔 32.4%。

4.3.5 刪除權行使的限制或擴張相對權重分析

刪除權行使的限制或擴張議題中，需評估權重的作法包含以下：

一、鼓勵刪除權擴張，行使被遺忘權。於個資法內明訂資料主體對於個人資料相關搜尋結果之刪除權，對搜尋引擎業者課以刪除之義務(以下簡稱：鼓勵刪除權擴張，行使被遺忘權)。

二、鼓勵刪除權擴張，但從嚴行使被遺忘權。訂定被遺忘權檢驗標準，如資料主體是否為公眾人物、內容侵害隱私程度等(以下簡稱：鼓勵刪除權擴張，但從嚴行使被遺忘權)。

三、限制刪除權擴張，不行使被遺忘權。為維護商業言論自由，維持現狀，不提供資料主體刪除已公開個人資料之權利(以下簡稱：限制刪除權擴張，不行使被遺忘權)。

表 4-10 刪除權行使的限制或擴張改善作法相對權重排序

構面	權重	排序
鼓勵刪除權擴張，行使被遺忘權。於個資法內明訂資料主體對於個人資料相關搜尋結果之刪除權，對搜尋引擎業者課以刪除之義務。	0.276	2
鼓勵刪除權擴張，但從嚴行使被遺忘權。訂定被遺忘權檢驗標準(如資料主體是否為公眾人物、內容侵害隱私程度等) 。	0.565	1
限制刪除權擴張，不行使被遺忘權。為維護商業言論自由，維持現狀，不提供資料主體刪除已公開個人資料之權利。	0.158	3
C.R.	0.002	
C.I.	0.001	
R.I	0.58	

資料來源：本研究整理

根據統計軟體分析結果，如表<4-10>，「鼓勵刪除權擴張，行使被遺忘權」相對權重值佔 27.6%，「鼓勵刪除權擴張，但從嚴行使被遺忘權」相對權重值佔 56.5%，而「限制刪除權擴張，不行使被遺忘權」相對權重值佔 15.8%。

4.3.6 問卷分析

一、去識別化與再識別風險

有專家將美國醫療法(HIPAA)之安全港準則與歐盟與美國簽訂之安全港原則混淆，即使目前歐盟-美國之安全港原則已廢除，目前以歐美隱私保護盾牌為雙方保護個人資料之依據，歐盟-美國之安全港原則尚於隱私法演進中重要一環，因此法律專家容易將美國醫療法(HIPAA)中的去識別安全港準則聯想為歐盟-美國之安全港準則。

除此之外，學者認為去識別化之技術規範定義不夠明確。值得一提的是，去識別化的標準我國目前為採用非強制性之 CNS 29191 作為去識別規範之標準。而國際最新隱私保護系統最新標準為英國標準協會於 2017 年 3 月 31 日發布之 BS 10012:2017，此系統係依照《一般資料保護規章》(GDPR)訂定之標準，其中去識別化要求即為必須以加入干擾之去識別方式，禁止以遮蔽或加入編碼之方式，此要求與本研究之實證研究結果互相呼應。

二、資料蒐集告知困境

法律專家認為必須闡明告知同意及告知的差別。我國目前個資法第 15 條[79]規定公務機關蒐集資料主體個人資料前須經過資料主體必須符合相關條件，其中之一為當事人之「同意」。而第 19 條[80]則規定非公務機關於蒐集或處理應有特定目的，並符合部分條件如與資料主體有契約關係或經由當事人同意等。

---

[79] 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
一、執行法定職務必要範圍內。
二、經當事人同意。
三、對當事人權益無侵害。

[80] 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
一、法律明文規定。
二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
五、經當事人同意。
六、為增進公共利益所必要。
七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

三、刪除權行使的限制或擴張

針對實證研究結果，部分學者認為「參照日本東京法院公布之被遺忘權標準」的方式尚存爭議。首先，日本於被遺忘權標準僅為判決書之定義，並尚成為成為判例。其次，需要探討若要訂定被遺忘權之標準，是否可能產生其他問題。如刪除標準產生爭議時，應如何處理、是否需要透過司法途徑以及應由何監督機構監督資料控制者？

先前研究亦有學者討論美國若要引進被遺忘權，須以何種方式引進。除此之外，亦指出監督機構於監督資料控制者上的爭議，如：搜尋引擎業者是否可能在無人申請刪除的情況下任意刪除公開資料(顏于嘉，2017)。

4.3.7 小結

在本次專家問卷所建立的大數據三大關鍵隱私議題中，「去識別化與再識別風險」佔整體權重的第一名，「資料蒐集告知困境」次之，且兩者權重相當接近。「刪除權行使的限制或擴張」最低，且權重相當低。AHP 層級分析法分析結果與 4.1.3 章節之修正式德爾菲法問卷統計結果相互呼應，修正式德爾菲法結果指出專家對於「刪除權行使的限制或擴張」看法一致性相對較低，看法極端。4.3.2 章節 AHP 層級分析法關鍵隱私議題分析結果近一步證實部分專家認為此議題之重要性相對權重較低。

於「資料蒐集告知困境」議題中，專家給予「以部門式立法排除告知適用」相對權重最高。而「以事後管理取代事前管理」相對權重最低，可見專家認為事後管理在實務上執行相對困難。

於「去識別化與再識別風險」議題中，專家給予「技術規範加以限制」相對權重最高，而「訂定去識別化之安全港準則」次之。

八、對當事人權益無侵害。
蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

於「刪除權行使的限制或擴張」議題中，專家給予「鼓勵刪除權擴張，但從嚴行使被遺忘權」相對權重最高。可見專家雖認同被遺忘權為世界趨勢需引進我國，但尚須嚴格執行之以免阻礙商業言論自由。

第五章 結論與建議

5.1 結論

隨著大數據應用的逐漸普及，相關應用對於隱私衝擊也逐漸浮出，如何兼顧應用與隱私是全球所面臨的共同問題。尤其各國國情及文化不同，如何在鼓勵大數據應用及促進經濟發展之前提下保護資料主體隱私權，成為更加複雜之議題。因此政府更應積極思考，但審慎處理個人資料保護法的修正，訂定一套適合我國，並同時維護大數據應用的發展並保障公民的隱私權的個人資料保護法。本研究目的為探討大數據世代下關鍵隱私議題及我國於各議題之改善方向，依本研究第三章各國對於各議題之相關政策及看法以及第四章專家問卷的結果分析，彙整以下結論：

一、瞭解資料保護政策

不論是否針對大數據發展下的個人資料保護，各國對於資料保護在過去皆有一定程度的概念，但各國對於資料保護的看法不一，因此作法亦不盡相同，如圖<5-1>並簡述如下：

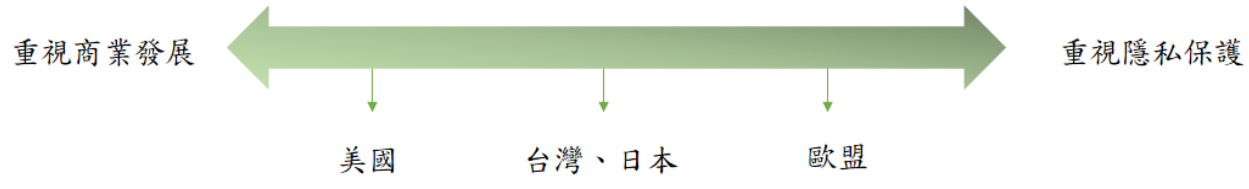


圖 5-1 商業發展及隱私權光譜

資料來源：本研究自行整理

1.歐盟

就隱私權重視程度而言，歐盟為隱私權保護的先驅，因此歐盟皆採取嚴格的資料保護機制，如：於資料蒐集告知皆採「選擇加入」模式、去識別化標準要求資料控制者刪除原始資料、明定被遺忘權賦予資料主體刪除自身公開個人資料之權利。

2.美國

美國則是相對重視商業發展及自由，因此採取較寬鬆的資料保護機制，如資料蒐集告知基本上採用「選擇退出」模式、去識別化標準僅以安全港準則為主，且基於美國憲法第一增修條文保障商業言論自由，被遺忘權難以於美國執行。

3.日本

日本目前由於「選擇退出」行之有年，且為保障「個資清冊業者」，對於資料蒐集告知尚採用「選擇退出」模式，但對業者課予之義務有逐漸嚴格之趨勢。去識別化之標準則與我國較為接近，若資料控制者或第三方無可比對之資料則屬去識別化資料，無須刪除原始資料。被遺忘權則雖於 2017 年 1 月被最高法院駁回，但東京法院已公布被遺忘權之執行標準。

4.台灣

我國對於資料蒐集之告知，目前與歐盟相同採「選擇加入」模式，相對較嚴格。去識別化標準目前則僅有較嚴格但不具強制力之國家標準，資料控制者不須刪除原始資料，但不得與其他資料相比對，間接識別之。被遺忘權則是尚未確立，亦無執行標準。

表 5-1 各國個人資料保護相關規範及現況

	歐盟	美國	日本	台灣
資料蒐集告知義務	採用「選擇加入」模式。	依產業而異，一般採用「選擇退出」模式。	採用「選擇退出」模式。	採用「選擇加入」模式。
去識別化標準	以三大標準檢驗，且須刪除原始資料。	以安全港準則為主，專家判斷為輔。	不得與其他資料比對間接識別，不須刪除原始資料。	不得與其他資料比對間接識別，不須刪除原始資料。
被遺忘權	已於《一般資料保護規章》(GDPR)中確立[81]。	尚未確立，且與美國憲法第一增修條文內容相牴觸。	尚未確立，但法院已公布檢驗標準。	尚未確立，且無檢驗標準。

資料來源：本研究自行整理

二、瞭解關鍵隱私議題

本研究以美國白宮所發布之三次《大數據白皮書》為基礎，找出大數據世代下關鍵議題，進一步透過文獻回顧探討各別議題。透過德爾菲專家問卷，結果指出除「分析結果引發偏誤與歧視」議題之外，專家認為「資料蒐集告知困境」、「去識別化與再識別風險」及「刪除權行使的限制或擴張」三者皆為大數據世代下關鍵隱私議題。重要程度則是「去識別化與再識別風險」最高，「資料蒐集告知困境」次之，且兩者權重皆相當高，「刪除權行使的限制或擴張」相對較低。

三、瞭解我國個人資料保護改善方向

1.資料蒐集告知困境

[81] 凡是已公開個人資料「不適當」或「無關連」或「已無關連且多餘」，而且「與公共利益無關」民眾就有權行使被遺忘權。

對於資料蒐集之告知義務，本研究透過專家問卷訪談，發現專家普遍認為參照美國作法，以「部門式」立法，訂定產業特別法，排除個資法告知義務適用範圍為適合我國兼顧大數據應用及隱私保護之作法。而「以事後管理取代事前管理」相對權重最低，可見專家認為事後管理在實務上執行相對困難。

2.去識別化與再識別風險

對於去識別化之標準，本研究透過專家問卷訪談，發現專家普遍認為我國較適合針對去識別技術加以限制，規定須以包含加入干擾之方式為之，如「雜訊加入」、「差分隱私」等。若採用此種技術規範方式，一般以遮蔽個人資料的方式，如「資料代碼化處理」、「取代」等方式，將不符合去識別化之標準。

3.刪除權行使的限制或擴張

對於被遺忘權，本研究透過專家問卷訪談，發現專家普遍鼓勵被遺忘權之行使，但須從嚴執行之，訂定相關檢驗標準。可見專家雖認同被遺忘權為世界趨勢需引進我國，但尚須嚴格執行之以免阻礙商業言論自由。

5.2 建議

本研究將透過上述結論，給予我國政府立法機構及業者相關建議，以符合本研究之研究目標。因此以下將分為政策意涵以及管理意涵，分別給予我國立法機構及大數據應用業者相關建議。

5.2.1 政策意涵

由於立法時間及資源有限，且商業自由及隱私權保護往往存在一定衝突，在此有限理性情況下，本研究根據 5.1 節之結論，給予立法機構相關建議如下：

一、重視「去識別化與再識別風險」及「資料蒐集告知困境」議題。

本研究認為在大數據世代下，本研究認為「去識別化與再識別風險」及「資料蒐集告知困境」兩大議題，除了大數據應用外，尚對於政府開放資料、處理個人資料爭議以及新型商業模式的推動皆有相當的影響，且根據 4.3.2 節與 5.1 節關鍵隱私議題構面分析及結論，專家認為此兩大議題之重要性相對較高，因此本研究建議我國立法機構可優先處理此兩大議題。

二、以「部門式」立法，排除個資法告知義務適用範圍。

針對資料蒐集告之義務，由於本研究認為我國立法機構參照美國立法，以「部門式」立法。但不同於美國為於各產業法中於業者課以告知義務，我國則建議於產業法中排除個資法告知義務適用範圍，於大數據分析需求高，應用相對普及之產業之產業法中增修特別法。如：我國目前保險法 177-1 條規定：「保險業為執行核保或理賠作業需要，處理、利用依法所蒐集保險契約受益人之姓名、出生年月日、國民身分證統一編號及聯絡方式，得免為個人資料保護法第九條第一項之告知。」即為得免為個人資料保護法第九條第一項之告知之案例。

三、建立去識別技術規範

關於去識別化標準機制的建立，我國目前是需以個案評估，視資料接受者識別能力而定。因此面對再識別風險，我國立法機構若無法明確定義「間接識別」，則可以技術規範方式，要求業者必須採用特定去識別技術。亦或可參照美國訂定去識別化之安全港準則，列出必須刪除之個資項目，刪除後即符合去識別化標準，若有特殊情況則輔以專家判斷。除此之外，本研究認為建立中立的第三方驗證機制輔以協助判斷資料控制者是否有侵害隱私權之虞。

四、賦予資料主體被遺忘權並建立檢驗標準

我國個人資料保護法中，並無賦予資料主體對於第三方於網路上發布之公開個人資料之刪除權，意即並未引進「被遺忘權」。但本研究認為被遺忘權之概念逐漸受到重視，尤其我國個人資料保護法受到歐盟法影響較深，且我國大法官釋字第509號解釋[82]指出，言論自由應兼顧隱私權，若為隱私保護，法律尚非不得對言論自由依其傳播方式為合理之限制。因此本研究建議立法機構於個人資料保護法增修資料主體對於第三方於網路上發布之公開個人資料之刪除權，如搜尋引擎之搜尋結果或新聞連結。然而，為平衡商業言論自由及隱私權，且「被遺忘權」之概念於我國尚未成熟，根據4.3.4節分析結果及5.1結論，亦建議立法機構可參照日本東京法院[83]，訂定檢驗標準[84]並從嚴執行之。

五、重視大數據所產生之歧視議題

由本研究實證研究發現，大數據分析結果引發偏誤與歧視議題尚未被重視，本研究認為歧視議題尚為大數據世代下隱私議題。因此，從預防方面，立法機構應積極於將設計著手保護隱私(privacy by design)[85]之概念法制化，於立法階段便將大數據

[82] 我國司法院大法官釋字第509號解釋：「言論自由為人民之基本權利，憲法第十一條有明文保障，國家應給予最大限度之維護，俾其實現自我、溝通意見、追求真理及監督各種政治或社會活動之功能得以發揮。惟為兼顧對個人名譽、隱私及公共利益之保護，法律尚非不得對言論自由依其傳播方式為合理之限制。」

[83] 日本平成28年45號判決

[84] 參照本文3.3.3

[85] Ann Cavoukian 提出七大「設計著手保護隱私」原則(Privacy by design)(郭戎晉，2013; Cavoukian, 2009)：

一、 應化被動為主動，並防範於未然。而非事後亡羊補牢。

二、 使隱私成為預設機制

所產生的歧視問題納入考量，加以規範之。另外，大數據分析進行階段可參照美國《公平信用報告法》(Fair Credit Reporting Act)，以法律明確規範大數據分析的程序、提升大數據演算法之透明性。最後，若歧視問題產生，亦可參照美國以行政管制方式，授權公平交易委員會監督業者，並於《公平交易法》中訂定相關規範救濟方法，並由公平交易委員會執行之，提供資料主體此一救濟管道。

三、 於設計中植入隱私
四、 完整的機能：正和而非零和
五、 環環相扣的安全：貫穿資料生命週期的保護
六、 能見度與透明度：保持開放性
七、 尊重用戶隱私：確保以用戶為中心

5.2.2 法律意涵

本研究根據 5.1 節之結論，給予明確修法建議如下：

一、「刪除權行使的限制或擴張」修法建議

對於「刪除權行使的限制或擴張」，本研究建議於我國個資法第 11 條補充「當公開之個人資料與公共利益無關，則應依當事人得請求依照事實性質及內容、隱私侵害範圍及程度、公開之目的、當事人社會影響力及社會狀況評估是否得以刪除之。」

二、將資訊保護專責機構納入法規要求，要求公、私部門設立資訊保護官。

我國立法院於 2017 年提出資訊長四法並一讀通過，本研究建議除了公務機關須設立資訊總處以外，也應要求非公務機關設立資訊保護單位，向主管機關回報業者是否確實遵守個人資料保護相關規範，以因應國際最新隱私保護系統最新標準 BS 10012:2017。然而，依照比例原則，為避免造成小型企業成本過高，歐盟 GDPR 草案之標準，只要求員工人數於 250 以上之企業設立資料保護單位，並向主管機關負責[86]。但由於台灣中小企業居多，員工人數 250 以上之企業比例相對較低，因此本研究認為可參照經濟部中小企業處公布之中小企業處法規認定標準，員工人數低於 100 人為中小企業，相對員工人數 100 人之大型企業即應設立資料保護單位以保護資料主體之權利。抑或可針對使用個人資料之數量較多或敏感性資料較多之產業進行要求，如電信業、金融業存有龐大客戶資料、醫療業存有客戶敏感性資料。

5.2.3 管理意涵

本研究主要探討業者於大數據應用及資料主體隱私權之權衡，且本研究專家問卷所發放之對象多屬業界人士，因此於大數據應用之業者而言，尚有其參考價值，本研究根據 5.1 節之結論，給予業者建議如下：

一、簡化個人資料蒐集告知之內容。

[86]歐盟後來將此前提修正，凡是有個人資料蒐集、處理歐盟人民之企業皆須遵守 GDPR 之規範。

諸多文獻指出一般消費者對於隱私權政策或服務條款不甚了解，或是內容過於複雜，導致資訊不對稱獲知識落差問題，且歐盟於 2016 年通過之《一般資料保護規章》(GDPR)開始要求業者以簡明扼要的方式於個人資料蒐集時進行告知義務。因此本研究建議業者於蒐集個人資料時盡量以簡明扼要知方式進行告知義務。亦可參考歐盟的三個基本要素：隱私政策必須有三個基本要素：其必須簡潔易懂、須用淺顯的語言清楚寫明，使即便是孩童也能理解、應為免費服務。

二、加強去識別之技術

本研究發現專家傾向贊成以技術規範作為去識別化之標準，且目前我國已正在推行國家標準 CNS 29191 亦屬嚴格之技術規範。雖然我國目前並無強制業者以特定技術進行個人資料的去識別化，但本研究認為技術規範為目前去識別發展之趨勢，因此建議業者加強去識別技術，並於提供給第三方時注意第三方之再識別能力。

三、確保大數據分析程序合理

雖目前大數據應用下「分析結果引發偏誤與歧視」之問題尚不受重視，但本研究認為，此議題之嚴重性即在於其難以被社會大眾所關注，業者亦容易忽視其大數據應用尚可能引發偏誤或歧視。因此本研究建議業者應確保大數據應用程序合理、演算法是否客觀。

5.3 後續研究建議

本研究探討大數據世代下隱私關鍵議題，包含四大議題，分別為「資料蒐集告知困境」、「去識別化與再識別風險」、「刪除權行使的限制或擴張」以及「分析結果引發偏誤或歧視」。本研究雖已透過嚴謹的研究方法探討我國面臨各關鍵議題之改善方向，但因時間等因素限制，並無法進一步深入探討具體作法，故對後續研究有下列之建議。

一、個人資料蒐集之「部門式」立法

由於各產業之性質不同，建議後續研究可深入探討我國各產業對於個人資料蒐集的需求及分別的潛在隱私風險，進一步將具體之修法建議提供政府參考，作為立法依據。

二、去識別化標準之技術規範

不同之去識別化技術對於業者成本、資料主體隱私保障及執行難度皆有差異，過與不及皆非立法機構所樂見，因此該以何種技術規範做為我國之強制性標準，建議後續研究可進一步探討之。

三、被遺忘權之檢驗標準

由於目前我國對於被遺忘權尚不適法，且相關學術研究尚屬不多，建議後續研究可於被遺忘權執行檢驗標準多做著墨，以較為溫和之方式將被遺忘權引進我國個資法中。另外，亦可探討被遺忘權引進後之監督議題，例如我國是否須以司法途徑之方式監督資料控制者。

四、大數據分析結果偏誤與歧視問題

雖本研究透過文獻回顧及專家問卷，皆發現大數據分析結果所產生偏誤與歧視問題目前並未受到重視，但本研究認為大數據應用開始滲透人民生活，這些包裝在客觀分析下的歧視會造成嚴重的社會問題。從美國 2014 年至 2016 年逐年發布之《大數據白皮書》之脈絡可發現，美國越來越重視此議題。因此建議後續研究深入探討大數據分析結果偏誤與歧視之問題，例如我國若要將「從著手設計保護隱私 (Privacy by design)」法制化，具體作法為何。

參考文獻

中文書籍

王玉民(1994)。***社會科學研究方法原理***。洪葉文化出版股份有限公司。

阮綠茵、管倖生、王明堂、王藍亭、李佩玲(2007)。***設計研究方法***.。全華圖書。

沈瑞棋、施東河、勝助(1998)。***應用灰關聯分析於旅遊風險評估模式之研究。灰色系統理論與應用***。建國技術學院。

羅世宏、蔡欣怡、薛丹琦(2008)。***質性資料分析：文本、影響與聲音***。五南圖書出版股份有限公司。

趙國棟、易歡歡、糜萬軍、鄂維南(2014)。***大數據時代***。五南圖書出版股份有限公司。

洪德欽、陳淳文(2015)。***歐盟法之基礎原則與實務發展(上)***。國立臺灣大學出版中心。

中文期刊

謝文和(2003)。***博物館成人學習之研究建構主義觀點－以國立臺灣史前文化博物館(博士論文)***。國立臺灣師範大學社會教育學系研究所，台北市。

呂雅惠(2007)。***企業內電子郵件監控與隱私權保護爭議之探討(碩士論文)***。國立政治大學法學院在職專班，台北市。

黃昭元(2012)。***論差別影響歧視與差別對待歧視的關係***。*中研院法學期刊*, 11。

郭戎晉(2013)。***隱私法制新趨勢-從設計著手保護隱私(Privacy by Design)***。*科技法律透析*,, 25(8), 38-44。

翁清坤(2013)。***告知後同意與消費者個人資料之保護***。*臺北大學法學論叢*, (87)。

蔡博坤(2013)。***智慧聯網時代巨量資料法制議題研析-以美國隱私權保護為核心***。*科技法律透析*, 25(10)。25(10), 46-62。

劉定基(2013)。***析論個人資料保護法上［當事人同意］的概念***。*月旦法學雜誌*, (218)。146-167。

范姜真媺(2014)。***歐盟及日本個人資料保護立法最新發展之法務部委託研究案成果報告***。東海大學，台中市。

謝依彣(2014)。***因應物聯網之[自設計著手保護隱私]概念法制化之研究(碩士論文)***。國立清華大學科技法律研究所，新竹市。

李進建(2015)。***論大數據於犯罪偵查之挑戰與因應***。*中華民國全國律師期刊*, 12, 60-69。

葉志良(2016)。***大數據應用下個人資料定義的檢討：以我國法院判決為例***。*資訊社會研究*。31, 1-36。

蔡昀臻、樊國楨(2016)。***大數據之資料去識別的標準化實作初探: 根基於 ISO/IEC 2nd WD 20889: 2016-05-30***。*資訊安全通訊*, 22(4), 1-26。

蔡昀臻、樊國楨(2016)。***個人資料管理系統標準化初論: 根基於個人資料去識別化之議題***。*資訊安全通訊*, 22(1), 1-27。

楊柏宏、陳鈰雄(2016)。***被遺忘權之研析-以歐盟法院 Google Spain SL 案及歐盟個資保護規章為中心***。*萬國法律*, (208), 98-120。

郭戎晉(2016)。***日本個人資料保護法修正重點與去識別化推動剖析***。*科技法律透析*, *28*(6), 43-52。

王自雄(2016)。***從美國就巨量資料之管制現況與立法趨勢論我國可能之因應對策***。*科技法律透析*, 28(2), 30-52。

匡文波、黃琦翔. (2016)。***大數據熱的冷思考***。國際新聞界, 38(8), 134-148。

我國法務部(2016)。***全國法規資料庫「個人資料保護法」***。

張志偉(2017)。***記憶或遺忘，抑或相忘於網路－從歐洲法院被遺忘權判決，檢視資訊時代下的個人資料保護。****政大法學評論*, (148), 1-68。

張玉宏、秦志光、肖樂(2017)。***大數據算法的歧視本質***。*自然辯證法研究*, (5), 81-86。

彭金隆、陳俞沛、孫群。(2017)。***巨量資料應用在台灣個資法架構下的法律風險***。*臺大管理論叢*, *27*(2), 93-118。

林玫君(2017)。***論個人資料保護法之[當事人同意]***。*東海大學法學研究*, (51), 121-170。

陳聰富、蔡甫昌(2017)。***大數據應用於醫學研究之法律議題***。*台灣醫學*, 21(1), 34-42。

樓一琳、何之行(2017)。***個人資料保護於雲端運算時代之法律爭議初探暨比較法分析: 以健保資料為例***。*臺大法學論叢*, *46*(2), 339-422。

翁清坤(2017)。***商業言論自由與個人資料保護之衝突：以美國電信業與我國金控業個人資料流通之管制為中心***。*臺大法學論叢*, *46*(3), 703-799。

吳珞齊(2017)。***The Conflicts Between The Applications of Big Data and Personal Information Protection Act in Taiwan-Take Insurance Industry as an Example***。*電腦稽核*, (35), 60-79。

顏于嘉(2017)。***由美國資訊隱私法制觀察被遺忘權在美國的發展***。*萬國法律*, (211), 25-33。

李思瑩(2016)。***論被遺忘權之保障及經濟分析(碩士論文)***。中國文化大學法律學系，台北市。

王慕民、陳品安、吳彥欽、張又丹(2015)。***「通訊傳播事業個人資料保護之機制及管理模式」委託研究報告***。達文西個資暨高科技法律事務所。

中文網路文獻

裴洪輝(2014)。***美國推「橡皮擦法案」抹掉未成年人的網路過失***。法律與生活 2014 年第 1 期。取自 http://doc.qkzz.net/article/452df124-df17-49b6-8a9e-ef2150d083f6.htm (最後瀏覽日：2018/06/13)

資策會(2014)。***科技法治應用***。科技法律電子報 2014 年 9 月。取自 https://stli.iii.org.tw/epaper_hx.aspx?auid=699 (最後瀏覽日：2018/06/13)

李科逸(2014)。***歐盟 2014 個人資料保護日，倡議資料可攜權及個資規範革新***。資策會科技法律研究所。2016 年 10 月。取自 https://stli.iii.org.tw/pdf.aspx?url=https%3A%2F%2Fstli.iii.org.tw%2Farticle-detail.aspx%3Fno%3D65%26tp%3D1%26i%3D144%26d%3D6469%26prn%3Dy (最後瀏覽日：2018/06/14)

胡湘湘(2014)。***大數據藏金礦，銀行業挖商機***。台灣銀行家 2014 年 11 月。取自 https://www-07.ibm.com/tw/dp-cs/smartbanking/pdf/Cover_story4_big_data.pdf (最後瀏覽日：2018/07/16)

傅志華(2015)。***大數據在金融業的應用。***數位行銷實戰家 2015 年 1 月。取自 https://blog.dcplus.com.tw/marketing-knowledge/growther/24648 (最後瀏覽日：2018/06/14)

張立翹(2015)。***被遺忘權制度框架及引入中國的可行性***。Dimen.net 迪蒙資訊中心網 2015 年 2 月 28 日取自 http://www.dimeng.net/news/content-21882-26.html (最後瀏覽日：2018/06/14)

陳曉莉(2015)。***適用於 28 個會員國的歐盟新資料保護法出爐了***。IThome 2015 年 12 月 16 日。取自 http://www.ithome.com.tw/news/101551 (最後瀏覽日：2018/06/14)

台灣人權促進會(2015)。***我的行車紀錄，你的開放資料？鑽法律漏洞，政府大量開放人民資料***。資訊新聞中心。2015 年 10 月 23 日。取自 http://www.tahr.org.tw/node/1656 (最後瀏覽日：2018/07/16)

宋佩珊(2015)。***美國發布了「消費者隱私權法」草案***。資策會科技法律研究所 2016 年 10 月。取自 https://stli.iii.org.tw/pdf.aspx?url=https%3A%2F%2Fstli.iii.org.tw%2Farticle-detail.aspx%3Fno%3D64%26tp%3D1%26i%3D148%26d%3D6852%26prn%3Dy (最後瀏覽日：2018/06/14)

彭子豪、胡漢朝(2015)。***資誠：全球逾六成企業應用大數據作決策***。經濟日報 2015 年 1 月 28 日。取自 http://www.pwc.tw/zh/news/media/media-20150128-7.html (最後瀏覽日：2018/07/16)

朱雲鵬、陳金隆(2015)。***如何促進大數據在台灣的發展***。國政評論 2015 年 5 月 29 日。取自 http://www.npf.org.tw/1/15081 (最後瀏覽日：2018/06/14)

呂雪慧(2015)。***政院推大數據，三產業先行***。中時電子報 2015 年 4 月 8 日。取自 http://www.chinatimes.com/newspapers/20150408000035-260202 (最後瀏覽日：2018/06/14)

金元浦(2016)。***「大數據時代」的美國隱私保護制度***。一點資訊 2016 年 5 月 20 日。取自 http://www.yidianzixun.com/article/0DLqs0yW (最後瀏覽日：2018/06/15)

我是二姐夫(2016)。***歐盟是如何通過立法來保護個人數據隱私的***。鈦媒體 2016 年 1 月 13 日。取自 http://www.tmtpost.com/1497640.html (最後瀏覽日：2018/06/15)

聶家音(2016)。***歐盟將頒布一般資訊保護規章***。台灣經貿網 2016 年 4 月 15 日。取自 http://www.twcsi.org.tw/international detail.php?Iid=3239 (最後瀏覽日：2018/07/26)

陳文義(2016)。***IDC:全球大數據分析市場 2019 年將達 1870 億美元***。iThome 2016 年 5 月 24 日。取自 http://www.ithome.com.tw/news/106166 (最後瀏覽日：2018/06/15)

彭宏傑、柳雁軍、李瀟璇(2016)。***告訴你，被遺忘權存在驚天大 BUG***！騰訊研究院 2016 年 3 月 24 日。取自 https://read01.com/zh-tw/7K4M3N.html#.WfMlN2iCzIU (最後瀏覽日：2018/06/15)

我國法務部 (2016)。***公務機關利用去識別化資料之合理風險控制及法律責任***。2016 年 10 月 21 日取自 https://training.ndc.gov.tw/upload/ofiles/20161021090832.pdf (最後瀏覽日：2018/06/15)

甄美玲(2016)。***在一片爭議聲中，「被遺忘權」在歐盟確立和實施***。傳媒透視 2016 年 6 月 16 日。取自 http://gbcode.rthk.org.hk/TuniS/app3.rthk.hk/mediadigest/content.php?aid=2071 (最後瀏覽日：2018/06/15)

最极客(2016)。***大數據帶來的隱私洩漏和歧視問題漸顯，數據發展正面臨轉折點***。香港矽谷 2016 年 3 月 14 日。取自 http://www.hksilicon.com/articles/1035281

蔣哲宇(2017)。***日最高院，首定義網路「被遺忘權」***。資策會科技法律研究所 2017 年 2 月。取自 https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=156&d=7737 (最後瀏覽日：2018/06/15)

王宏仁(2017)。***產學界呼籲政府先推動資訊長四法，義美食品總經理高志明更直言：國家資訊政策不明，設政府 CIO 才能問責***。iThome 2017 年 6 月 9 日。取自 https://www.ithome.com.tw/news/114849 (最後瀏覽日：2018/06/15)

英文文獻

Aggarwal, A. (2016). Identification of quality parameters associated with 3V's of Big Data. *Computing for Sustainable Global Development*, pp.1135-1140. *IEEE*.

Armstrong, D., Kline-Rogers, E., Jani, S. M., Goldman, E. B., Fang, J., Mukherjee, D. & Eagle, K. A. (2005). Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome. *Archives of Internal Medicine*, 165(10), pp.1125-1129.

Benitez, K., Loukides, G., & Malin, B. (2010). Beyond safe harbor: automatic discovery of health information de-identification policy alternatives. *Proceedings of the 1st ACM International Health Informatics Symposium*, pp.163-172.

Cate, F. H. (2006). The failure of fair information practice principles. *Consumer Protection in the Age of the Information Economy*, pp.1-15

Cavoukian, A., & Castro, D. (2014). Big Data and innovation, setting the record straight: De-identification does Work. *White Paper*, Jun, 20, pp.1-13.

Clemons, E. K., & Hitt, L. M. (2000). The Internet and the Future of Financial Services: Transparency: Differential Pricing and Disintermediation, *Wharton School Center for Financial Institutions*, University of Pennsylvania, pp.1-39

Cranor, L. F., Arjula, M., & Guduru, P. (2002). Use of a P3P user agent by early adopters. *In Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, pp.1-10.

Davenport, T. H., & Dyché, J. (2013). Big data in big companies. *International Institute for Analytics*, pp.1-31

Farrell, H. (2003). Constructing the international foundations of e-commerce—The EU-US Safe Harbor Arrangement. *International Organization*, 57(2), 277-306.

Garfinkel, S. L. (2015). De-identification of personal information. *National Institute of Standards and Technology*, 8053, pp.1-46.

Gilbert, F. (2015). The right of erasure or right to be forgotten: what the recent laws, cases, and guidelines mean for global companies. *Journal of Internet Law*, 18(8), pp.1-20.

Hirsch, D. D. (2014). That's Unfair-Or Is It: Big Data, Discrimination and the FTC's Unfairness Authority. *Kentucky Law Journal* 103, pp.345.

Holden, M. C., & Wedman, J. F. (1993). Future issues of computer-mediated communication: The results of a Delphi study. *Educational Technology Research and Development*, 41(4), pp.5-24.

Hsu, P. F., & Chen, B. Y. (2007). Developing and implementing a selection model for bedding chain retail store franchisee using Delphi and fuzzy AHP. *Quality and Quantity*, 41(2), pp.275-290.

Jensen, M. (2013). Challenges of privacy protection in big data analytics. *2013 IEEE International Congress*, pp.235-238. *IEEE*.

Kim, K. D., & Choi, K. (2012). A Study on the Policy of Sustainable Domestic Timber Supply Using Delphi Technique and AHP. *Journal of Korean Forestry Society*, 101(3), pp.434-442.

King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer–Privacy concerns when behavioural advertisers target mobile phones–Part I. *Computer Law & Security Review*, 26(5), pp.455-478.

King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer–Is industry self-regulation adequate to protect consumer privacy when behavioural advertisers target mobile phones?–Part II. *Computer Law & Security Review*, 26(6), pp.595-612.

Koops, B. J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice. *SCRIPTed*, 8, pp.1-28.

Kraus, J. L. (1993). On the Regulation of Personal Data Flows in Europe and the United States. *Colum. Bus. L. Rev.*, pp.59.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4), pp.372-386.

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, 38(11), pp.1134-1145.

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2012). The challenge of 'big data' for data protection. *International Data Privacy Law*, 2(2), pp.47-49.

Liao, C. N. (2010, July). Supplier selection project using an integrated Delphi, AHP and Taguchi loss function. *In Probstat Forum*, pp.118-134.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), pp.336-355.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, 29(3), pp.229-235.

Matturdi, B., Zhou, X., Li, S., & Lin, F. (2014). Big Data security and privacy: A review. *China Communications*, 11(14), pp.135-145.

Mundie, C. (2014). Privacy Pragmatism; Focus on Data Use, Not Data Collection. *Foreign Affairs*., 93, pp.28.

Munoz, C., Smith, M., & Patil, D. (2016). *Big data: A report on algorithmic systems, opportunity, and civil rights*. Executive Office of the President. The White House.

Murry Jr, J. W., & Hammons, J. O. (1995). Delphi: A versatile methodology for conducting qualitative research. *The Review of Higher Education*, 18(4), 423-436.

Narayanan, A., Huey, J., & Felten, E. W. (2016). A precautionary approach to big data privacy. In *Data protection on the move*, pp. 357-385.

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA law review*, 57, pp.1701.

Party, D. P. W. (2007). Opinion 4/2007 on the concept of personal data. Brussels, *Belgium: European Commission*.

Rapport, D. J., & Maffi, L. (2013). A Call for Integrative Thinking. *Science*, 339(6123), 1032-1032.

Ratti, C., Frenchman, D., Pulselli, R. M., & Williams, S. (2006). Mobile landscapes: using location data from cell phones for urban analysis. *Environment and Planning B: Planning and Design*, 33(5), 727-748.

Raut, R. D. (2014). An integrated Delphi-AHP-DEA-LPP multi criteria decision making approach for supplier selection and order quantity allocation system. *International Journal of Logistics Systems and Management*, 18(3), 366-393.

Rosen, J. (2012). The right to be forgotten. *Stanford law review online*, 64, 88.

Rubinstein, I. (2012). Big data: the end of privacy or a new beginning?. *International Data Privacy Law (2013 Forthcoming)*, 12-56.

Rubinstein, I. S., Lee, R. D., & Schwartz, P. M. (2008). Data mining and Internet profiling: Emerging regulatory and technological approaches. *The University of Chicago Law Review*, 75(1), pp.261-285.

Saaty, T. L. (1980). Analytic hierarchy process. John Wiley & Sons, Ltd.

Sakshaug, J. W., Schmucker, A., Kreuter, F., Couper, M. P., & Singer, E. (2016). Evaluating active (opt-in) and passive (opt-out) consent bias in the transfer of federal contact data to a third-party survey agency. *Journal of Survey Statistics and Methodology*, 4(3), pp.382-416.

Schmidt, A., Paradiso, J., & Noble, B. (2011). Automotive pervasive computing. *IEEE Pervasive Computing*, 10(3), pp.12-13.

Supakkul, S., Zhao, L., & Chung, L. (2016). GOMA: Supporting Big Data Analytics with a Goal-Oriented Approach. In *Big Data (BigData Congress), 2016 IEEE International Congress on*, pp.149-156.

Sweeney, L. (2000). Simple demographics often identify people uniquely. Health (San Francisco), 671, pp.1-34.

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, 11, xxvii.

Vidal, L. A., Marle, F. & Bocquet, J. C. (2011). Using a Delphi process and the Analytic Hierarchy Process (AHP) to evaluate the complexity of projects. *Expert systems with applications*, *38*(5), pp.5388-5405.

Wheeller, B., Hart, T. & Whysall, P. (1990). Application of the Delphi technique: A reply to Green, Hunter and Moore. Tourism Management, 11(2), pp.121-122.

Weiss, M. A. & Archick, K. (2016). US-EU Data Privacy: From Safe Harbor to Privacy Shield. Congressional Research Service.

Woodcock, R. A. (2017). Big Data, Price Discrimination, and Antitrust. *Hastings Law Journal*, *68*(6), 1371.

Xue, M., Magno, G., Cunha, E., Almeida, V. & Ross, K. W. (2016). The Right to be Forgotten in the Media: A Data-Driven Study. *Proceedings on Privacy Enhancing Technologies*, 2016(4), 389-402.

英文書籍

Gostin, L. O., Levit, L. A., & Nass, S. J. (2009). *Beyond the HIPAA privacy rule: enhancing privacy, improving health through research.* National Academies Press.

Huang, C. S., Lin, Y. J., & Lin, C. C. (2008). Evaluation models for choosing insurance policy using the AHP, Fuzzy Logic, and Delphi Technique. *WSEAS International*

Conference. Proceedings. Mathematics and Computers in Science and Engineering (No. 7). World Scientific and Engineering Academy and Society.

Saaty, T. L. (2013). Analytic hierarchy process. In *Encyclopedia of operations research and management science* (pp. 52-64). Springer, Boston, MA.

英文報告書

Party, D. P. W. (2007). Opinion 4/2007 on the concept of personal data. Brussels, *Belgium: European Commission*.

United States. Executive Office of the President & Podesta, J. (2014). *Big data: Seizing opportunities, preserving values*. White House, Executive Office of the President.

United States. Executive Office of the President & Podesta, J. (2015). *Big data: Seizing opportunities, preserving values*. White House, Executive Office of the President.

英文網路文獻

Brill, J. (2012). Big data, big issues. *Fordham University School of Law*. Retrieved from http://www.ftc.gov/public-statements/2012/03/big-data-big-issues (最後瀏覽日：2018/06/16)

Cecilia, K. (2017). Congress Move to Strike Internet Privacy Rule From Obama Era. *The New York Times*. Retrieved from https://www.nytimes.com/2017/03/23/technology/congress-moves-to-strike-internet-privacy-rules-from-obama-era.html (最後瀏覽日：2018/06/17)

Chiba, O. (2015). No judicial standard yet in Japan over right to be forgotten. In *The Asahi shimbun.* Retrieved from http://www.asahi.com/ajw/articles/AJ201608240007.html (最後瀏覽日：2018/06/17)

Daniels, B. L. (2013). Big data, big trouble? Privacy and legal concerns with big data. *Pillsbury Winthrop Shaw Pittman LLP.* Retrieved from http://www.lexology.com/library/detail.aspx?g=027d46af-e621-4714-8da4-27c07f7ee6e0 (最後瀏覽日：2018/06/16)

Denvil, J. & Kane, P. (2015). Insights on the Consumer Privacy Bill of Rights Act of 2015. In *Hogan Lovells*. Retrieved from http://www.hldataprotection.com/2015/03/articles/consumer-privacy/insights-on-the-consumer-privacy-bill-of-rights-act-of-2015/ (最後瀏覽日：2018/06/17)

Depczyk, J. (2010). A Different Game: Information is Transforming Traditional Businesses. *The Economist*. Retrieved from http://www.economist.com/node/15557465 (最後瀏覽日：2018/07/08)

Drozdiak, N. & Schechner, S. (2015). EU Court Says Data-Transfer Pact with U.S. Violates Privacy. *Wall Street Journal.* Retrieved from http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361 (最後瀏覽日：2018/06/17)

Drum, K. (2013). *Privacy is dead. Long live transparency!* In *Mother Jones.* Retrieved From http://www.motherjones.com/politics/2013/10/ future-of-privacy-nsa-snowden (最後瀏覽日：2018/06/16)

Fonseca, B. (2008). Unstructured data at risk in most firms, survey finds. Computerworld. In *Computerworld.* Retrieved from http://www.computerworld.com/article/2534496/datacenter/unstructured-data-at-risk-in-most-firms–survey-finds.html (最後瀏覽日：2018/06/16)

Gartner (2015). Gartner Survey Shows More Than 75 Percent of Companies Are Investing or Planning to Invest in Big Data in the Next Two Years. Retrieved from http://www.gartner.com/newsroom/id/3130817 (最後瀏覽日：2018/06/17)

IBM (2013). The Four V's of Big Data. Retrieved from http://www.ibmbigdatahub.com/infographic/four-vs-big-data (最後瀏覽日：2018/06/16)

ISACA. (2014). Generating value from big data analytics. *White Paper.* Retrieved from http://www.isaca.org/Knowledge-Center/Research/ ResearchDeliverables/Pages/Generating-Value-From-Big-Data-Analytics.aspx (最後瀏覽日：2018/06/16)

Kelion, L. (2015). Facebook data transfers threatened by Safe Harbour ruling. *BBC News.* Retrieved from http://www.bbc.com/news/technology-34442618 (最後瀏覽日：2018/06/17)

McKinsey Global Institute (2011). Big data: The next frontier for innovation, competition, and productivity. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation (最後瀏覽日：2018/06/16)

Normandeau, K. (2013). Beyond volume, variety and velocity is the issue of big data veracity. *Inside Big Data*. Retrieved from https://insidebigdata.com/2013/09/12/beyond-volume-variety-velocity-issue-big-data-veracity/ (最後瀏覽日：2018/07/24)

Sam, S. (2016). France Fines Google Over Right to be Forgotten. The *Wall Street Journal.* Retrieved from http://www.wsj.com/articles/france-fines-google-over-right-to-be-forgotten-1458847256（最後瀏覽日：2018/06/16)

Tung, L. (2013). Sweden tells council to stop using Google Apps. Zdnet. Retrieved from http://www.zdnet.com/sweden-tells-council-to-stop-using-google-apps-7000016850/ (最後瀏覽日：2018/06/16)

Yadron, D. (2014). Target hackers wrote partly in Russian, displayed high skill, report finds. In *The Wall Street Journal.* Retrieved from http://online.wsj.com/news/articles/SB10001424052702304419104579324902602426862 (最後瀏覽日：2018/06/16)

附錄一　修正式德爾菲法專家問卷

諸位專家先進您好:

非常感謝您撥冗填答此問卷,本研究之問卷是關於建構『大數據世代下我國現行隱私保護之改善方向』的研究方法,目的係在了解您對大數據應用下目前隱私相關議題研究構面，本研究為了避免議題過於發散，透過修正式德爾菲法初步以文獻分析方式蒐集四個大數據應用下相關議題，分別為 1.**去識別化與再識別風險**、**2.刪除權的行使或限制**、**3.分析結果引發偏誤與歧視**及 4.**蒐集告知困境**，以期作為層級分析法(Analytic Hierarchy Process,AHP)之架構，您所填寫的答案與提供的資料，僅供本研究彙整分析之用，感謝您撥冗填寫惠賜卓見，衷心期盼並感謝您對本研究之熱心協助。

敬祝　萬事如意

國立成功大學交通管理科學系電信管理研究所碩士班

指導教授　黃郁雯　博士

研 究 生　巫昱德　敬上

壹、基本資料

一、服務機構：

二、職稱：

三、專業領域：

貳、問卷內容

1. 再識別化風險

國際上一般見解認為，個人資料經過去識別化後，將因無法以合理可能方式識別出特定資料主體，故可迴避個資法之規範。而傳統之「去識別化」方式為將個人識別性資料去除僅保留數據，但研究顯示透過不同數據間比對，可將不包含個資之數據透過交叉比對再識別出特定個人，因此仍衍生個資疑義。

2. 刪除權的行使或限制

有學者認為數據應用之價值，在於累積大量之數據並從中分析，因此大數據與資料蒐集最小化有相違背之處(Tene & Polonetsky, 2012)，應摒棄資料最小化原則，加以限制資料主體之刪除權，才得以發揮大數據應用最大價值。

另一方面，部分學者認為大數據世代下第三方更容易取得資料主體的個人資料，認為刪除權應擴張於第三方於網路上發布資料主體個人資料之相關資訊，如資料主體對搜尋引擎要求其相關資訊刪除之(Ohm, 2011; Rosen, 2012)，此概念即為歐盟目前執行之被遺忘權，為刪除權的權利擴張。

3. 大數據分析結果錯誤與歧視問題

2016 年 5 月，美國白宮公布了第三次大數據報告，「Big Risks, Big Opportunities: the Intersection of Big Data and Civil Right」，指出大數據分析由於資料來源不盡完善，無法判斷所獲得的數據資料是否母體特性相符，這些本身含有偏誤的資料輸出之結果可能無意間將歧視特定公民。如白宮報告提及之案例，美國大學以大數據分析預估學生之畢業比例，結果指出，家庭收入是影響學生畢業比率之關鍵因素，低收入家庭學生退學比例較高，此結果可能使大學傾向拒絕招收低收入家庭的學生。單從分析結果來看，容易產生低收入家庭的學生能力不足的誤解，但大多低收入家庭的學生中途退學的原因是無法負擔高額學費，並非是能力不佳。大學運用大數據分析卻忽略其中的因果關係，最終造成對低收入家庭學生的歧視性結果。

4. 蒐集告知困境

(1).告知成本高

由於大數據的大量性特徵，業者難以一一告知資料主體，告知與取得授權的過程可能會產生巨量成本(Jensen, 2013)，尤其當現今行動裝置螢幕愈來愈小的趨勢，可呈現的資訊內容有限，告知任務將更加困難(Tene & Polonetsk, 2012)。

(2).對告知內容認知不足

美國醫學研究機構 IOM 於 2009 年報告指出由於因業者所提供之服務條款或隱私權政策通常較為複雜，消費者亦未必了解其意涵，故可能引發認知不足、知識落差或資訊不對稱之問題，使得告知實際上無法達到保護資料主體的目的，反而僅是將責任轉移轉至消費者。

請問您認為上述四個議題是否能代表大數據應用下隱私研究的重要議題，本問卷以李克特(Likert)五點尺度測量，請就其代表性分別以 1 到 5 分分別表示非常不同意、不同意、無意見、同意及非常同意。**除此些議題外，您認為是否有其他與大數據應用相關重要之隱私議題，請填寫於意見欄**。

	非常不同意 1 分	不同意 2 分	無意見 3 分	同意 4 分	非常同意 5 分
去識別化與再識別風險					
刪除權行使的限制或擴張					
分析結果引發偏誤與歧視					
資料蒐集告知困境					

意見欄：

附錄二　AHP 層級分析法問卷

諸位專家先進您好:

非常感謝您撥冗填答此問卷。本問卷是關於建構『大數據世代下我國現行隱私保護之改善方向』的研究問卷，目的在於了解您對我國大數據應用與隱私權保護改善方向之看法。

為確立並篩選驗究主題，本研究先前已透過『修正式德爾菲法』彙整出三大隱私議題，分別為「去識別化與再識別風險」、「刪除權行使的限制或擴張」、「資料蒐集告知困境」。現階段，本研究將依『層級分析法』蒐集各位專家對於此三大議題及各項做法之意見與權重分數。

問卷填答進行，採權重計分方式。首先，本問卷將會逐項說明各大議題及其可能的改善方向或做法，請各位專家就各項做法議題，根據您的專業判斷與經驗，給予兩兩相對重要性(或合適性)之權重比較，請參考下述 <一、填答方式說明>。

請您注意，本問卷填表目前所呈現的評估構面與準則排列，並不具有任何相對重要性或權重的意義，您的填答內容才會決定各項相對重要性與後續權重之計算結果。

本問卷蒐集您的專業意見，內容並不涉及任何個人私密資料。所有調查結果僅供學術研究，不做其他用途，敬請安心作答。您寶貴意見是本研究能夠順利完成的重要關鍵，在此先向您致上衷心的感謝。

若有任何問題，敬請不吝聯絡。

敬祝 萬事如意 身體健康

成大電信管理研究所研究生: 巫昱德 敬上

一、 填答方式說明

本研究之填答方式以兩兩比較方式進行，每次比較採 5 個等級，以 1-9 分計算權重。請您依專業判斷，綜合實務與學理分析，提供您的寶貴意見。

(1) 舉例而言: 請您比較指標 A1 與指標 A2，若您認為 A1 與 A2 同等重要，則請於 <同等重要(1)> 之欄位處填 v 如下。

指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
A1									v									A2

(2) 若您認為 A1 相對於 A2 重要，且「極重要(7)」，則請於 <極重要(7)>之處填 v 如下

指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
A1			v															A2

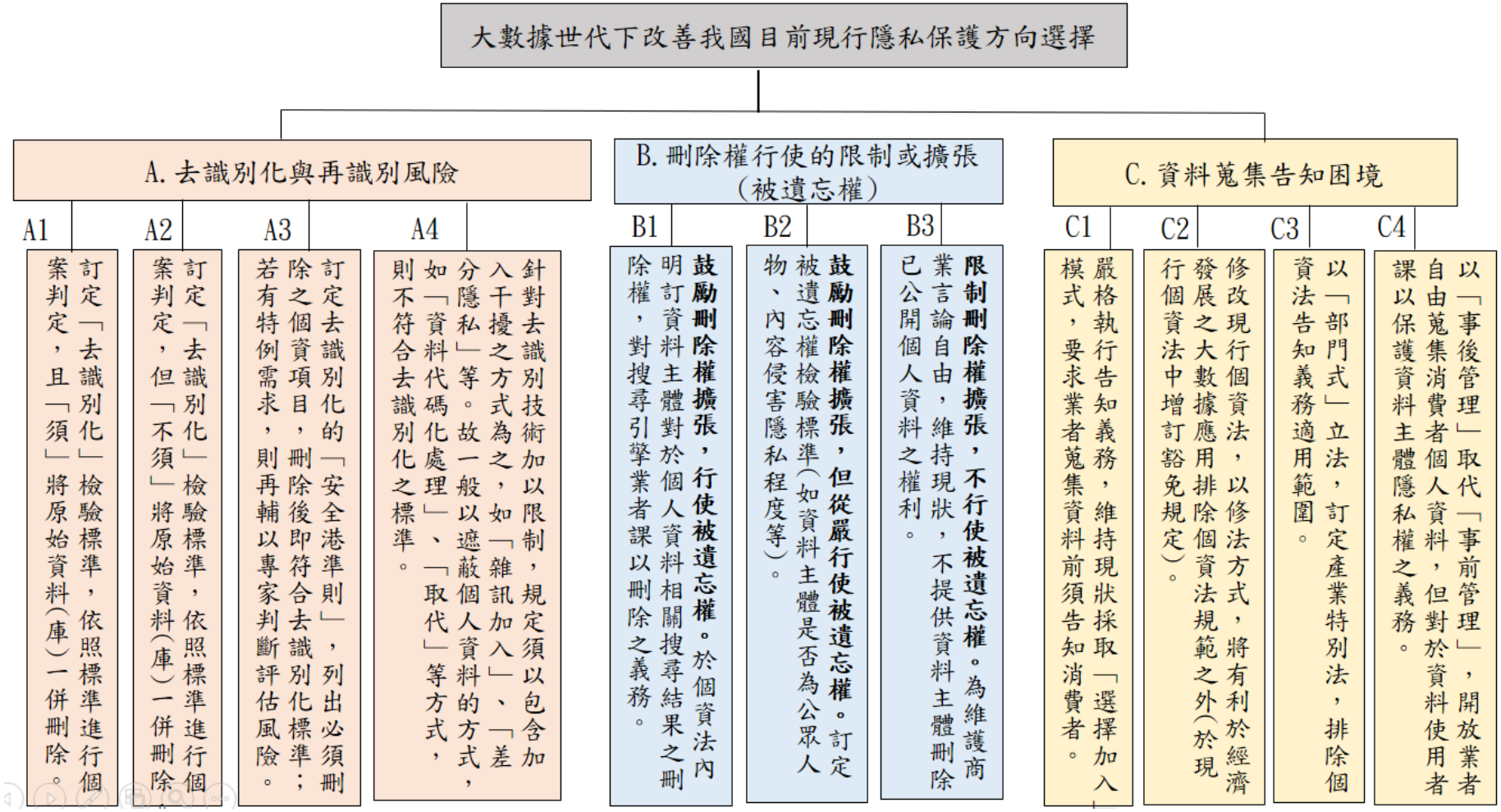
(3) 若您認為 A1 相對 A2 重要，且介於「極重要(7)」及「頗重要(5)」之間，請於 6 之處填 v 如下

指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
A1				v														A2

(4) 然而，若您認為 A2 相對 A1「稍重要(3)」，則請於「稍重要(3)」之處填 v 如下

指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
A1											v							A2

二、　本研究層級分析之架構圖



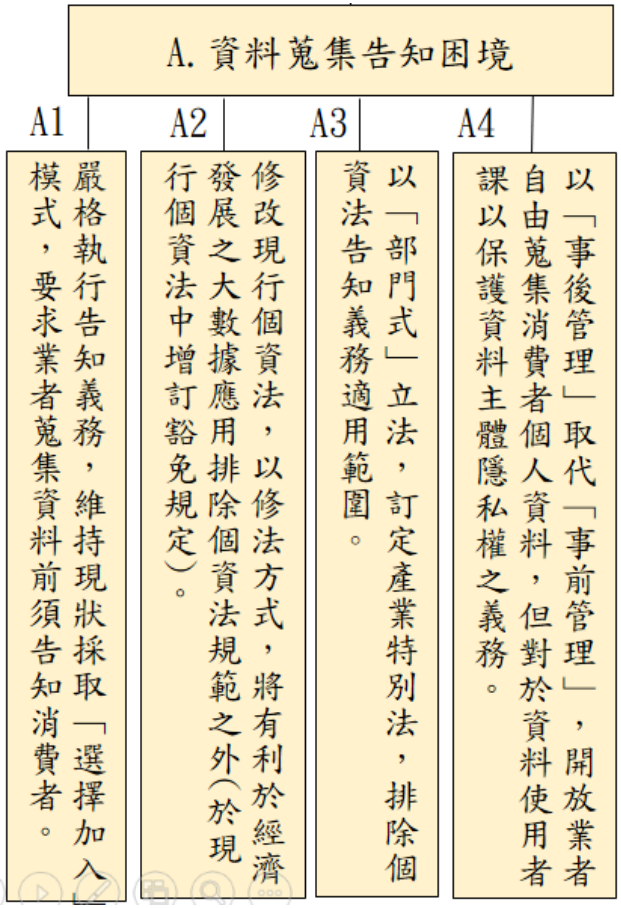
三、問卷填答

(1) 各個議題比較

因應大數據發展，隱私與個資保護正面臨挑戰。本研究彙整上述 **A**、**B**、**C** 三大議題分析相應之道，請您評估以 **A**、**B**、**C** 三項議題因應我國大數據發展的可行性與適用性，並就 **A**、**B**、**C** 三項議題之相對重要性權重(含可行性、適用性與改善之迫切程度)給予比較。

X指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	Y指標
	9	8	7	6	5	4	3	2	1	2	3	1	5	6	7	8	9	
(A)去識別化與再識別風險																		(B)刪除權的行使或限制(被遺忘權)
(A)去識別化與再識別風險																		(C)資料蒐集告知困境
(B) 刪除權的行使或限制(被遺忘權)																		(C)資料蒐集告知困境

(2) 議題 A.資料蒐集告知困境



議題概說: 對於資料之蒐集，根據現行個資法規定，台灣目前是以「選擇加入」(opt-in)模式，亦即業者在蒐集資料前須告知資料主體方可蒐集。但由於大數據的大量性特徵，業者難以一一告知資料主體，且告知的過程可能會產生巨量成本。但若以「選擇退出」(opt-out)模式，即業者得自由蒐集消費者個人資料，但消費者有要求停止蒐集之權利，此種模式對資料主體的保護程度則相對較低。

<作法 1>：對於資料蒐集的告知，歐盟與台灣的法律皆**以「選擇加入」為主，亦即個人資料的蒐集與利用，必須告知當事人之後，方可進行。(A1)**

<作法 2>：為解決現行個資法要求告知義務之困境，有學者認為**可將有利經濟發展之大數據應用排除現行個資法規範之外，如增修個資法第 51 條豁免適用範圍，或增修個資法第 8 條蒐集告知義務，增加豁免適用範圍。(A2)**

<作法 3>：美國則是以「部門式」立法，將蒐集資料之告知義務各別納入各產業相關法規中。若欲參照美國法，則可**訂定產業特別法，並於其中排除個資法告知義務。(A3)**

<作法 4>：另有有學者 (Mayer-Schönberger and Cukier, 2013)主張**以「事後管制」取代「事前管制」，開放業者可自由蒐集消費者個人資料而不須事前告知，但對於業者及資料使用者則課以隱私保護之義務，若消費者(資料主體)受到隱私侵害，則可請求損害賠償**。

本研究彙整四項作法(A1-A4)，請就此四項作法以**適合我國執行之程度**作為重要性評估標準，給予權重分數。

本議題之權重填答，請您比較 A1 與 A2、A1 與 A3、A1 與 A4、A2 與 A3、A2 與 A4、A3 與 A4，共 6 組比較。

X指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	Y指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
(A1) 嚴格執行告知義務，維持現狀採取「選擇加入」模式，要求業者蒐集資料前須告知消費者。																		(A2) 修改現行個資法，以修法方式，將有利於經濟發展之大數據應用排除個資法規範之外(於現行個資法中增訂豁免規定)。
(A1) 嚴格執行告知義務，維持現狀採取「選擇加入」模式，要求業者蒐集資料前須告知消費者。																		(A3) 以「部門式」立法，訂定產業特別法，排除個資法告知義務適用範圍。
(A1) 嚴格執行告知義務，維持現狀採取「選擇加入」模式，要求業者蒐集資料前須告知消費者。																		(A4) 以「事後管理」取代「事前管理」，開放業者自由蒐集消費者個人資料，但對於資料使用者課以保護資料主體隱私權之義務。

X指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	Y指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
(A2) 修改現行個資法，以修法方式，將有利於經濟發展之大數據應用排除個資法規範之外(於現行個資法中增訂豁免規定)																		(A3) 以「部門式」立法，訂定產業特別法，排除個資法告知義務適用範圍
(A2) 修改現行個資法，以修法方式，將有利於經濟發展之大數據應用排除個資法規範之外(於現行個資法中增訂豁免規定)																		(A4) 以「事後管理」取代「事前管理」，開放業者自由蒐集消費者個人資料，但對於資料使用者課以保護資料主體隱私權之義務
(A3) 以「部門式」立法，訂定產業特別法，排除個資法告知義務適用範圍																		(A4) 以「事後管理」取代「事前管理」，開放業者自由蒐集消費者個人資料，但對於資料使用者課以保護資料主體隱私權之義務

(3) 議題 B.去識別化與再識別風險

議題概說: 國際上一般見解認為，個人資料經過『去識別化』後，將難以合理可能方式再識別出特定資料主體，故可藉由將個人資料去識別化，來迴避個資法之規範。傳統的「去識別化」方式為將個人識別性資料去除，僅保留數據，或改換成資料代碼或亂碼。但若干研究顯示，去識別化資料，透過不同數據間的交叉比對，仍有可能再識別出特定個人，因而衍生出『再識別之風險』與個資保護疑義。針對去識別化與再識別風險，各國有提出不同的因應之道與做法，概述如下。以下請教專家，有何看法，並請兩兩比較，給予權重分數。

<作法 1> 對於去識別化與再識別風險，歐盟目前做法為，**訂定『去識別化』檢驗標準**(主要檢驗『去識別化』後，是否仍可能識別資料主體、是否可與其他資料相連、是否仍可推論出特定人相關)」，**依照個案判定是否達到此標準，另外，並要求將原始資料一併刪除(B1、B2)**

<作法 2> 美國『去識別化』的檢驗方式為**訂定「安全港準則」，列出必須刪除的個資項目，(例如：姓名、帳戶號碼、電話號碼等)，刪除後即符合『去識別化』標準；然而若有特例，或須進一步檢驗，則再輔以「專家判斷評估風險」，決定是否達到去識別化標準(B3)**

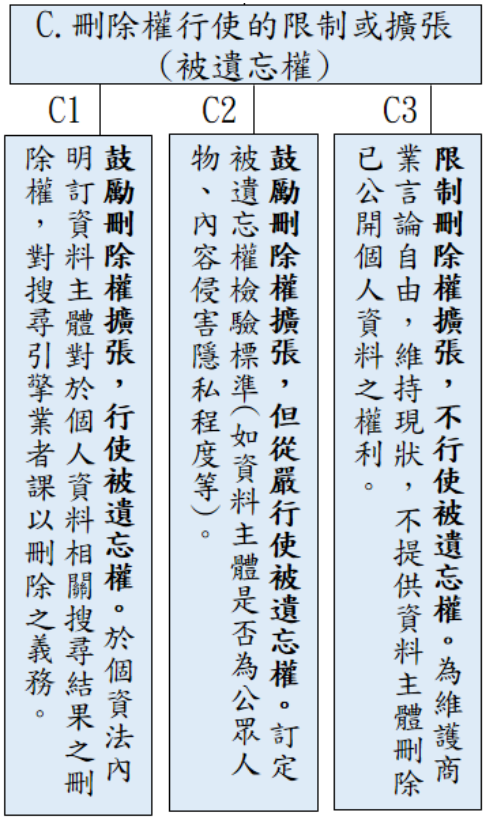
<作法 3> 亦有學者認為『去識別化』標準，可考慮**針對去識別技術加以限制，須以特定技術為之，例如加入特定干擾技術(「雜訊加入」、「差分隱私」等)，藉此以達去識別效果。反之，一般以遮蔽個人資料的方式，例如「資料代碼化處理(Pseudonymisation)(Token)」、「取代(Substitution)」等方式，則因未加入特定干擾技術，故不符合去識別化之標準(B4)**。

本研究彙整四項作法(B1-B4)，請就此四項作法以**適合我國執行之程度**作為重要性評估標準，給予權重分數。
本議題之權重填答，請您比較 B1 與 B2、B1 與 B3、B1 與 B4、B2 與 B3、B2 與 B4、B3 與 B4，共 6 組比較。

X指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	Y指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
(B1) 訂定「去識別化」檢驗標準，依照標準進行個案判定，且「**須**」將原始資料(庫)一併刪除。																		(B2) 訂定「去識別化」檢驗標準，依照標準進行個案判定，但「**不須**」將原始資料(庫)一併刪除。
(B1) 訂定「去識別化」檢驗標準，依照標準進行個案判定，且「**須**」將原始資料(庫)一併刪除。																		(B3) 訂定去識別化的「安全港準則」，列出必須刪除之個資項目，刪除後即符合去識別化標準；若有特例需求，則再輔以專家判斷評估風險。
(B1) 訂定「去識別化」檢驗標準，依照標準進行個案判定，且「**須**」將原始資料(庫)一併刪除。																		(B4) 針對去識別技術加以限制，規定須以包含加入干擾之方式為之，如「雜訊加入」、「差分隱私」等。故一般以遮蔽個人資料的方式，如「資料代碼化處理」、「取代」等方式，則不符合去識別化之標準。

X指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	Y指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
(B2) 訂定「去識別化」檢驗標準，依照標準進行個案判定，但「**不須**」將原始資料(庫)一併刪除。																		(B3) 訂定去識別化的「安全港準則」，列出必須刪除之個資項目，刪除後即符合去識別化標準；若有特例需求，則再輔以專家判斷評估風險。
(B2) 訂定「去識別化」檢驗標準，依照標準進行個案判定，但「**不須**」將原始資料(庫)一併刪除。																		(B4) 針對去識別技術加以限制，規定須以包含加入干擾之方式為之，如「雜訊加入」、「差分隱私」等。故一般以遮蔽個人資料的方式，如「資料代碼化處理」、「取代」等方式，則不符合去識別化之標準。
(B3) 訂定去識別化的「安全港準則」，列出必須刪除之個資項目，刪除後即符合去識別化標準；若有特例需求，則再輔以專家判斷評估風險。																		(B4) 針對去識別技術加以限制，規定須以包含加入干擾之方式為之，如「雜訊加入」、「差分隱私」等。故一般以遮蔽個人資料的方式，如「資料代碼化處理」、「取代」等方式，則不符合去識別化之標準。

(4) 議題 C.刪除權的行使或限制(被遺忘權)



議題概說: 數據應用之價值，在於累積大量之數據並從中分析。因此大數據的蒐集與應用與個資法所強調之「資料蒐集最小化原則」恐有相違背之處，故有學者主張應摒棄「資料蒐集最小化原則」，並進一步限制資料主體之刪除權，才得以發揮大數據蒐集與應用的最大價值，同時亦是維護商業言論自由之作法。然而，亦有學者認為大數據世代下，透過搜尋引擎的搜尋功能，個人資料在網路上的取得與散布更加迅速，故有主張「資料刪除權」應擴及於第三方於網路上發布之個人資訊，例如對搜尋引擎 Yahoo、Google 等要求刪除搜尋結果之連結，此概念即為歐盟目前所執行之「被遺忘權」，可視為「資料刪除權」的擴張。對於資料刪除權的限制或擴張，各國作法歧異，分述如下。

<作法 1> 對於刪除權行使的限制或擴張，歐盟目前**於個資法規範內明確賦予資料主體對於個人資料相關『連結』的刪除權(亦稱作「被遺忘權」)。凡是內容已無存在必要，且與公共利益無關，資料主體則可對搜尋引擎行使刪除權(被遺忘權)。(C1)**

<作法 2> 日本對於刪除權之擴張採從嚴辦理，例如根據 2017 年東京法院判決提出，須**以特定檢驗標準判定刪除權擴張與否 (如資料主體是否為公眾人物、內容侵害隱私程度等)，唯有保護隱私權的價值明顯高於資訊公開才得以行使被遺忘權。(C2)**

<作法 3> 亦有學者認為應參照美國**維護言論自由及資訊流通，主張維持現狀不提供資料主體刪除已公開個人資料之權利。(C3)**

本研究彙整被遺忘權行使之各國作法(C1-C3)，請就此三項作法，以**適合我國執行之程度**作為重要性評估標準，給予權重分數。本議題之權重填答，請您比較 C1 與 C2、C1 與 C3、C2 與 C3，共 3 組比較。

X指標	絕對重要		極重要		頗重要		稍重要		同等重要		稍重要		頗重要		極重要		絕對重要	Y指標
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
(C1) **鼓勵刪除權擴張，行使被遺忘權。**於個資法內明訂資料主體對於個人資料相關搜尋結果之刪除權，對搜尋引擎業者課以刪除之義務。																		(C2) **鼓勵刪除權擴張，但從嚴行使被遺忘權。**訂定被遺忘權檢驗標準(如資料主體是否為公眾人物、內容侵害隱私程度等)。
(C1) **鼓勵刪除權擴張，行使被遺忘權。**於個資法內明訂資料主體對於個人資料相關搜尋結果之刪除權，對搜尋引擎業者課以刪除之義務。																		(C3) **限制刪除權擴張，不行使被遺忘權。**為維護商業言論自由，維持現狀，不提供資料主體刪除已公開個人資料之權利。
(C2) **鼓勵刪除權擴張，但從嚴行使被遺忘權。**訂定被遺忘權檢驗標準(如資料主體是否為公眾人物、內容侵害隱私程度等)。																		(C3) **限制刪除權擴張，不行使被遺忘權。**為維護商業言論自由，維持現狀，不提供資料主體刪除已公開個人資料之權利。

基本資料

服務機構：

職稱：

專長或專業領域：

填表日期：

四、意見與建議

非常歡迎您提供任何有關大數據應用與資料保護的相關意見或建議，或不吝給予任何研究建議、評論或指導。

對於本問卷若有任何建議或評論，也請您不吝提供。長短不拘，衷心感謝。

問卷結束，非常感謝您對本研究的支持與填答。